jamk.fi

Barona I.C.T Poland kriittisten laitteiden verkonvalvonta

Topi Rytkönen

Opinnäytetyö
Joulukuu 2015
Tekniikan ja liikenteen ala
Ohjelmistotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Rytkönen Topi	Opinnäytetyö, AMK	7.12.2015
	Sivumäärä 57	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Barona I.C.T Poland kriittisten laitteiden verkonvalvonta

Tutkinto-ohjelma
Ohjelmistotekniikan koulutusohjelma

Työn ohjaaja(t)
Mika Rantonen

Toimeksiantaja(t)
Barona ICT Services Poland

Tiivistelmä

Baronan Puolan toimipiste on ICT-palveluratkaisuja tarjoava palvelukeskus. Toimeksiantaja tarvitsi jo olemassa olevan verkkomonitoroinnin tueksi tarkemman ja helpommin saatavilla olevan verkkovalvontaratkaisun pääpainon ollessa Puolan toimipisteessä. Yritys oli jo valmiiksi hankkinut Qentinel NetEye nimisen verkkomonitorointiohjelman, jota ei kuitenkaan ollut vielä otettu käyttöön. Tehtävänä oli ottaa käyttöön tämä kyseinen järjestelmä ja lisätä valvontaan Puolan toimipisteen kannalta kriittisiä laitteita. Tavoitteena ei ollut täydellisen verkkovalvonnan toteuttaminen jokaisesta mahdollisesta laitteesta, vaan pikemminkin hyvän pohjan luominen, minkä avulla valvontaa voidaan tulevaisuudessa helposti laajentaa.

Valvontaa lähdettiin toteuttamaan ensin tutustumalla verkonvalvontaan käsitteenä ja hankkimalla pohjatietoa monitoroinnin teoriasta ja käytänteistä. Aiheeseen tutustumisen jälkeen alettiin kartoittamaan NetEyen mahdollisuuksia työkaluna ja suunnittelemaan itse valvottavien laitteiden lisäämistä valvontaan. Laitteet valittiin pääasiassa sillä kriteerillä, että laitteiden tulee olla nimenomaan Puolan toimipisteen toiminnan kannalta kriittisessä asemassa. Lopulta valvontaan lisättäviä laitteita tuli yhteensä 10 kappaletta, joista 5 oli palvelimia ja 5 eri tietoverkkolaitteita.

Toteutus tehtiin yhteistyössä kolmannen osapuolen kanssa, joka toimi välikätenä verkkolaitteisiin. Yrityksen verkkojärjestelyt olivat sen verran arkaluontoisia, että itse laitteiden konfiguraatioon ei ollut valvontaa tehdessä suoraa pääsyä. Kun valvottavat laitteet oli valittu ja päätös käytetyistä mittareista tehty, oli seuraavana vuorossa laitteiden lisäys NetEyen valvonnan piiriin. Kaikki halutut laitteet ja testit lisättiin, ja hälytyksien raja-arvot määritettiin käyttäen NetEyen käyttöliittymää. Lisäksi määritettiin toiminta vikatilanteissa ja käyttäjäkohtaiset näkymät kustomoitiin halutun kaltaisiksi.

Valvonta saatiin toteutettua, kuten oli tavoitteena. NetEye soveltuukin verkkomonitorointiin hyvin helppokäyttöisyyden ja kustomoitavuuden vuoksi. Valvontaan saatiin lisättyä tarpeelliset laitteet ja Puolan toimipisteen verkon yleistilannetta on nyt helppo tarkastella NetEyen avulla.

Avainsanat (asiasanat)
Verkonvalvonta, verkkomonitorointi, SMNP, MIB, ICMP, NetEye

Muut tiedot

jamk.fi

Kuvailulehti

Author(s)	Type of publication	Päivämäärä
Rytkönen Topi	Bachelor's thesis	7.12.2015
	Number of pages 57	Language of publication:
		Permission for web publication: x

Työn nimi

Barona I.C.T Poland Monitoring of critical devices

Degree programme

Software Engineering

Supervisor(s)

Mika Rantonen

Assigned by

Barona ICT Services Poland

Description

The Polish office of Barona is a service center providing different levels of ICT -support in various situations. The company already had some level of network monitoring, however, the employer needed more coverage on top of the existing system, the main focus being on the Polish office. The company had already acquired a network monitoring software called Qentinel NetEye, but it had not been used nor configured yet. The task was to deploy and configure that said software and to monitor devices, critical for the Polish service center. The goal was not to monitor every single device possible, but to create a good foundation for future expanding.

The implementation was started by first getting familiar with the subject in general and getting some basic knowledge on theory and practices of network monitoring. After gathering some basic knowledge on the topic it was time to add the required devices to NetEye itself, which was done by first getting familiar with NetEye as a monitoring tool, and secondly by deciding which devices to actually monitor. The criteria for the devices was that they are important for the functioning of the Polish office. At the end, 10 devices were added of which 5 were servers and 5 were different network devices.

The implementation was carried out in cooperation with a third party, which operated as a middleman to the network devices. This was needed because the network arrangement was quite delicate, therefore a direct access to the monitored devices was not possible. After the devices for the monitoring were decided, and the decision of how these devices were to be tested, it was time to add these devices for monitoring using NetEye. All the desired devices and tests were added, alert thresholds configured and user depended views set.

The monitoring was carried out as planned, and NetEye did serve well as monitoring software because of its user friendliness and customizability. All the wanted devices were added to NetEye successfully, and overall viewing the situation of the Polish service center network via NetEye is now an easy task.

Keywords (subjects)

Network monitoring, SNMP, MIB, ICMP, NetEye

Miscellanous

Sisältö

Kuviot

Taulukot

Lyhenteet

ASN.1	Abstract Syntax Notation One
CPU	Central Processing Unit
FCAPS	Fault, Configuration, Accounting, Performance, Security
ICMP	Internet-Control Message Protocol
ICT	Information and Communications Technology
IP	Internet Protocol
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KPI	Key Performance Indicator
LAN	Local Area Network
MIB	Management information base
MPLS	Multiprotocol Label Switching
OID	Object Identifier
OSI	Open Systems Interconnection
PING	Packet Internet Groper
PDU	Protocol data unit
SLA	Service Level Agreement
SMI	Structure of Management Information
SMS	Short message service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

1. Lähtökohdat

1.1 Toimeksiantaja: Barona ICT Services Poland

Barona Group Oy on vuonna 1999 perustettu suomalainen yritys, joka tarjoaa henkilövuokraus ja suorarekrytointihenkilöstöpalveluita. Myös erilaiset ulkoistamispalvelut, Forenom-majoituspalvelut sekä Momentous suorahakupalvelu kuuluu Baronan tarjoamiin palveluihin. Vuosittain Barona työllistää noin 12 500 ihmistä logistiikka-, teollisuus-, rakennus-, toimisto-, IT- sekä sosiaali- ja terveystoimialan tehtäviin. Tällä hetkellä Barona toimii Suomen lisäksi Ruotsissa, Venäjällä, Virossa, Espanjassa ja Puolassa. (Barona yrityksenä n.d.)

Tarkemmin tämän työn toimeksiantajana oli Baronan Puolan yksikkö: Barona I.C.T Services Poland. Tämä palvelukeskus on Baronan ICT-palveluratkaisujen puolella toimiva haara, ja se pystytettiin Puolaan syksyllä 2012. Palvelukeskuksessa tarjotaan pääsääntöisesti etätuen erinäisiä palveluita: ensimmäisen ja toisen asteen teknistä tukea, palvelimien valvontaa, sovellusten paketointia/jakelua ja tietoturvapalveluita. Tällä hetkellä palvelukeskuksella on noin 50 työntekijää jakautuneena edellä mainittuihin työtehtäviin. Suurin osa toimii eri service desk -tiimeissä. (ICT-palveluratkaisut N.d.)

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli ensisijaisesti saada laadukas ja toimiva verkkomonitorointiratkaisu toimeksiantajayritykselle. Kyseinen monitorointi on tarkoitus toteuttaa Qentinel NetEye-nimisellä palvelulla, jolla on tarkoitus valvoa ICT-palveluja, verkkoa

sekä antaa hyvä yleisnäkymä Baronan palvelukeskuksen ICT-palvelujen tuottamiseen liittyvien resurssien tilasta.

NetEye-palvelu on hankittu Baronalle tarpeellisena lisänä verkon valvontaan ja raportointiin, mutta sitä ei ole vielä millään muotoa otettu käyttöön tai konfiguroitu. Tämä työkalu on siis tarkoituksena ottaa käyttöön kaikkine ominaisuuksineen, ja näin saada tarkka kuva nimenomaan Puolan palvelukeskuksen kriittisimipien verkkolaitteiden ja palvelimien tilasta. Tarkoituksena ei tässä vaiheessa ole tehdä äärimmäisen laajaa valvontaa, vaan pääpainona on ennemminkin NetEyen käyttöönotto. Tätä kautta pyritään saamaan hyvä alusta valvonnan laajentamisella tulevaisuudessa. Monien NetEyen ominaisuuksien joukosta tärkeimpinä mainittakoon verkkoliikenteen laatu (vasteajat, pakettihävikki jne.), palvelimien valvonta (prosessorin/muistin/kovalevyjen käyttöasteiden ja päällä olon valvonta) ja kaiken valvonnan ja monitoroinnin tuloksista kattava raportointi. Lisäksi NetEye tarjoaa webkäyttöliittymälleen käyttäjäryhmäkohtaiset näkymät, joihin valvottavat kohteet saadaan liitettyä saman loogisen kokonaisuuden alle. Koko NetEyen hallintakonsoli kustomoidaan yrityksen tarpeita vastaan.

2. Verkonvalvonta

2.1 Yleistä

Tietoverkot ovat kriittisessä roolissa nykymaailmassa, kun puhutaan käytännössä mistä vain tietojärjestelmästä tai tietokonepohjaisesta ratkaisusta. Tänä päivänä suurin osa liikenteestä kulkee verkon yli, ja tietoverkkojen määrä ja monimutkaisuus tulee kasvamaan tulevaisuudessa vielä lisää. Kaiken kulkiessa verkon yli on myös verkon toiminnasta vastaavien laitteiden syytä toimia moitteetta. Verkossa tapahtuva häiriö tai katkos voi heti johtaa yrityksen kannalta ikäviin taloudellisiin tappioihin. Tämä verkkoliikenteen jatkuva kasvaminen ja monimutkaistuminen ovat luoneet yrityksille tarpeen verkonvalvonnalle.

Verkonvalvonnalla tarkoitetaan nimenomaan verkkolaitteiden valvontaa, eikä itse verkkoliikenteeseen puututa. Sisäisen verkkoliikenteen valvonta ja hallinta on oma osa-alueensa, ja siihen löytyvät kokonaan omat työkalunsa. Verkonvalvonta ei myöskään itsessään ota kantaa verkon tietoturvaan eikä pyri aktiivisesti parantamaan sitä. Käsitteenä verkonvalvonta on siis osana laajempaa verkonhallinnan kokonaisuutta.

Yritysmaailmassa verkonvalvonta on kriittinen ja välttämätön osa kaikkia tietoverkkoja. Valvomalla verkon laitteita pystytään estämään mahdollisesti suuria taloudellisia tappioita, ja toimiva verkonvalvonta onkin täysin välttämätön osa yrityksien tietoverkkoja, jos kyseessä on vähänkään laajempi kokonaisuus.

Pääasiallisesti verkonvalvonta koostuu kolmesta elementistä: ohjelmistosta (hoitaa itse valvonnan), valvottavasta laitteesta sekä protokollasta (suorittaa halutut kyselyt käytetyn ohjelmiston kautta). Verkonvalvonnalla ei siis ole tavoitteenakaan tietoturvan parantaminen tai verkkoliikenteen valvominen. Valvonnalla pyritään sen sijaan parantamaan verkon toimivuutta, helpottamaan virheiden havainnointia ja mahdollisista vioista toipumista.

Tietoverkoissa tapahtuvasta huimasta kehityksestä huolimatta verkonvalvonta on pysynyt tiukasti mukana osana yrityksien verkkoratkaisuja. Verkonvalvonta on kulkenut kehityksen mukana, ja nykyään valvottavia kohteita voi olla paikallisesta lähiverkosta aina älypuhelimiin saakka. Valvontaa voi tehdä kaikennäköisille ja kokoisille verkoille oli kyseessä sitten WAN (Wide Area Network), LAN (Local Area Network), VoIP (Voice Over Internet Protocol), MPLS-yhteys (Multiprotocol Label Switching) tai rautapuolelta esimerkkeinä mainittakoon kytkimet, reitittimet, palvelimet sekä työasemat. (Nash & Behr 2007.)

Verkonvalvonta on yksinkertaisuudessaan järjestelmä, joka valvoo kaiken aikaa verkkoa ja sen palveluita. Kun järjestelmä kohtaa verkossa ongelman tai poikkeaman, se välittää heti tämän tiedon halutulle taholle ennalta määrättyä kanavaa pitkin. Kyseinen hälytys lähetetään itse verkonvalvontasovelluksen lisäksi esimerksi sähköpostitse tai SMS-viestinä (Short message service) verkon ylläpitäjille, mutta myös monia muita tapoja on olemassa.

Verkkovalvonnan toteutusta voi lähestyä monella eri tavalla, ja tarkoitukseen tehtyjä ohjelmia sekä niiden lisäosia onkin lukemattomia määriä. Valvonnan voi toteuttaa useilla eri ohjelmilla ja protokollilla SNMP-protokollan (Simple Network Management Protocol) näytellessä niistä suurinta roolia.

2.2 Toteutusfilosofia

Yritysmaailman verkkoratkaisuja on hyvin monenlaisia ja -laajuisia, joten monitoroinnin toteutuksessakin on monia variaatioita. Monitorointi tuleekin suunnitella tapauskohtaisesti yrityksen tarpeiden ja verkkoratkaisujen mukaan. Organisaatiot ovat kehittäneet omia suosituksia ja standardeja valvonnan toteuttamiseksi, ja näistä käytetyin lienee ISO:n (International Organization for Standardization) FCAPS-malli.

2.3 FCAPS-malli

2.3.1 Yleistä

FCAPS (fault, configuration, accounting, performance, security) on verkkomonitorointimalli, joka kuuluu osana laajempaan verkonhallinnan kokonaisuuteen. Tämän mallin ISO loi yhteistyössä OSI-ryhmän (Open Systems Interconnection) kanssa, ja 90-luvulla se lopulta saavutti tämänhetkisen muotonsa ITU-T:n (International Telecommunication Union: Telecommunication Standardization Sector) muokkaamana.

Tämä akronyymi on yleisesti käännetty suomeksi kohtiin vian, käytön, suorituskyvyn ja turvallisuuden hallinta. Jokainen näistä kohdista on osana verkonvalvonnan kokonaisuutta suurimman painoarvon ollessa vikojen ja suorituskyvyn hallinnassa. (ISO/IEC 7498-4 1989, 2; ITU-T x.700 1992, 3.)

2.3.2 Vikojen hallinta

Verkonvalvonnassa vialla tarkoitetaan tilannetta, jossa laite tai järjestelmä epäonnistuu sille annetussa tehtävässä hetkellisesti tai pitkäaikaisesti. Vikojen hallinta tarjoaakin menetelmät vikojen havaitsemiseen, eristämiseen ja poikkeuksellisien tilanteiden korjaamiseen. Jotta virheet voidaan havaita ja tiedottaa eteenpäin, tulee verkon tilasta olla saatavilla jatkuvasta reaaliaikaista tietoa. ISO/IEC 7498-4 standardissa on määritelty vianhallinnan toiminnot seuraavasti (ISO/IEC 7498-4, 3):

a) virhelokien ylläpito ja tarkastelu
b) virhetilanteiden ilmaantuessa niiden hyväksyminen ja toimiminen
c) virheiden tunnistaminen ja jäljitys
d) diagnosoivien testien suorittaminen
e) vikojen korjaus.

2.3.3 Käytön laskenta/hallinta

Käytön laskenta koskee palveluntarjoajia ja yrityksiä pääasiassa laskutus mielessä. Verkon resursseja monitoroimalla saadaan tarkat tiedot verkon yli menevästä liikenteestä, minkä perusteella asiakasta voidaan laskuttaa.

Käytön laskennan rinnalle on otettu mukaan myös käytön hallinta, jolla tarkoitetaan verkon resurssien käytön tarkastelua ylimääräisen kuormituksen tai väärinkäytön valvomiseksi. Käyttäjien toimien tutkimisella voidaan siis ehkäistä tarpeetonta verkon kuormittamista ja mahdollistaa verkon tehokkaampi käyttö tulevaisuudessa. ISO/IEC 7498-4 standardissa on määritelty käytön laskennan toiminnot seuraavasti (ISO/IEC 7498-4, 3):

a) Tiedottaa käyttäjiä aiheutuvista kuluista tai käytetyistä resursseista
b) Mahdollistaa kirjanpidon rajojen asettamisen ja yhdistää laskutuksen käytettyihin resursseihin

c) Mahdollistaa kulujen yhdistäminen, kun useat eri resurssit suorittavat annettua tiedonvälityksen tavoitetta.

2.3.4 Kokoonpanon hallinta

Kokoonpanon hallinnan tehtävänä on ylläpitää, päivittää ja varmistaa laitteiden välisten riippuvuuksien toiminta. Palveluiden pysäyttäminen ja uudelleenkäynnistäminen manuaalisesti sekä ajastetusti kuuluu myös kokoonpanon hallinnan piiriin. Kaikista muutoksista ja laitteiden välisestä liikenteestä kerätään myös dataa.

Niin kuin englanninkielisessä nimessä ”Configuration management” tuleekin jo ilmi, on laitteiden välisten yhteyksien konfigurointi osana kokoonpanojen hallintaa. Järjestelmänvalvojalla tuleekin olla helppo tehdä verkon konfiguraatioihin muutoksia, sikäli kun verkkoon tulee uusia laitteita tai muita muutoksia on tarpeen tehdä. (Hautaniemi 1994, luku 2.4.)

ISO/IEC 7498-4 standardissa on määritelty kokoonpanon hallinnan toiminnot seuraavasti (ISO/IEC 7498-4, 3):

a) verkon rutiinioperaatioiden/toimintojen parametrien asettaminen
b) hallittavien laitteiden ja laitekokonaisuuksien nimeäminen
c) hallittavien laitteiden alustaminen ja sammuttaminen
d) tiedon kerääminen verkon tämänhetkisestä tilasta
e) verkon konfiguraatioiden muuttaminen.

2.3.5 Suorituskyvyn hallinta

Suorituskyvyn hallinta analysoi ja kerää tietoa verkon suorituskyvystä. Tämä tarkoittaa käytännössä tietojen keräämistä esimerkiksi verkon välityskyvystä, käyttöasteesta, liikennemääristä ja vasteajoista. Kun edellä mainittuja kohtia valvotaan aktiivisesti, pystytään mahdolliset ylikuormitukset kitkemään hyvissä ajoin pois ja kriittisiin ongelmiin reagoimaan nopeasti.

ISO/IEC 7498-4 standardissa on määritelty suorituskyvyn hallinnan toiminnot seuraavasti (ISO/IEC 7498-4, 3):

a) tilastollisen tiedon kerääminen
b) järjestelmän tilatietoja tallentavien lokitiedostojen ylläpito ja tarkastelu
c) järjestelmän suorituskyvyn määrittely normaalissa, sekä poikkeuksellisissa oloissa.

2.3.6 Turvallisuuden hallinta

Turvallisuuden hallinnalla pyritään estämään verkon ja sen laitteiden luvaton käyttö ja muutenkin kontrolloimaan laitteisiin pääsyä. Turvallisuuspuolellakin tärkeässä roolissa on tiedon tallentaminen lokeihin. Kaikki epäilyttävä ja vähemmän epäilyttävä tieto tallennetaan lokeihin ja näitä tietoja voidaan myöhemmin analysoida.

Turvallisuuden hallinta määrittää, kenellä ja mistä on oikeus päästä käsiksi eri laitteisiin ja niistä saataviin palveluihin. Tietokonejärjestelmien sisäisten käyttäjäryhmien oikeuksien hallinnoiminen ei siis ole osana verkon turvallisuuden hallintaa.

ISO/IEC 7498-4 standardissa on määritelty turvallisuuden hallinnan toiminnot seuraavasti (ISO/IEC 7498-4, 3):

a) turvallisuuspalveluiden ja mekanismien luonti, poisto ja hallinta
b) turvallisuuteen liittyvän tiedon jakaminen
c) turvallisuuteen liittyvien tapahtumien raportointi ja tiedottaminen

3. Verkonvalvontaprotokollat

3.1 Yleistä

Verkonvalvontaprotokollia on muutamia erilaisia ja niitä käytetään eri tilanteissa riippuen siitä, mitä halutaan tehdä. Jotkin protokollat ovat hyvin yksinkertaisia ja soveltuvat vain tietynlaisen valvonnan suorittamiseen, kun taas joillain protokollilla voidaan suorittaa todella monimutkaisiakin kyselyitä.

3.2 SMNP

3.2.1 Yleistä

SNMP SNMP (Simple Network Management Protocol) on TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla, ja se toimii UDP-protokollan (User Datagram Protocol) päällä. SNMP on kaikkein yleisimmin käytetty verkonvalvontaan liittyvä protokolla. Käytännössä jokainen verkonvalvontaa suorittava ohjelmisto käyttää tavalla tai toisella SNMP-protokollaa. (Hautaniemi 1994, luku 4.)

Protokollalla eli yhteyskäytännöllä tarkoitetaan käytäntöä, joka mahdollistaa tiedon välityksen laitteiden kesken. SMNP on tällainen protokolla ja se on tarkoitettu verkkolaitteiden kuten reitittimien kytkimien ja työasemien valvontaan.

SMNP kehitettiin jo 1988 ja siitä tuli välittömästi käytetyin verkonhallintaprotokolla. Ensimmäisen version SNMPv1:sen piti olla vain tilapäinen ratkaisu verkonhallinnalle, mutta paremman protokollan loistaessa poissaolollaan siitä tulikin pitkäaikainen ratkaisu, ja sitä käytetään yhä. SNMP:n kehitystä jatkettiin ensin toisella versiolla,

SNMPv2, ja myöhemmin vielä versiolla SNMPv3 (versio 3), joka on IETF:n (Internet Engineering Task Force) mukaan nykyinen SNMP standardi. (Mauro & Schmidt 2005, 19–21.)

3.2.2 Toimintaperiaate

SNMP:hen kuuluu neljä eri osaa, jotka ovat hallinta-asema, hallinta-agentti, hallinta-tietokanta MIB (management information base) ja verkonhallinnan yhteyskäytäntö (käytännössä siis SNMP). Hallinta-agentti on yleisesti juurikin se laite, jota halutaan valvoa (reititin, kytkin, tulostin, työasema yms.). Hallinta-agentin tulee tukea SNMP-protokollaa, jotta kyselyt menevät läpi. Nykyään kuitenkin käytännössä kaikki verkko-laitteet tukevat vähintään SNMPv1:stä, joten SNMP-tuen puolesta ongelmia harvemmin ilmenee. Hallinta-aseman päässä pyörii puolestaan sovellus, joka vastaa verkon-valvonnasta. Erilaisia verkonvalvontasovelluksia on nykyään lukemattomia määriä, ja vaihtoehtoja löytyy monista avoimen lähdekoodin sovelluksista maksullisiin versioihin. Hallintatietokanta on kanta, joka sisältää muuttujat hallittavista tai tarkkailtavista kohteista. SNMP keskustelee MIB:n kanssa saadakseen tiedon näistä muuttujista. (Mauro & Schmidt 2005, 22–23.) MIB:stä enemmän luvussa 3.4

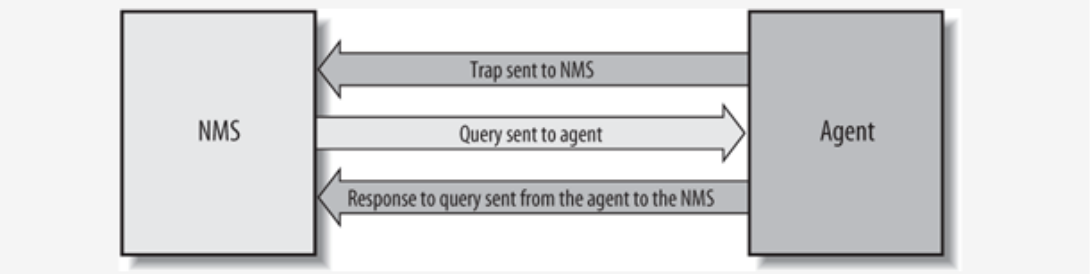
SNMP toimii UDP-protokollan päällä, mikä tarkoittaa, että myös SNMP on yhteydetön protokolla. Yhteydettömyys tarkoittaa, että hallintatyöaseman agentin välillä ei ole ylläpidettyä yhteyttä, vaan jokainen SNMP-viesti on oma erillinen tapahtumansa. Näin ollen verkkoon kohdistuva rasitus on varsin pientä, mutta SNMP-viestien perillemenosta ei ole varmuutta, ja viestejä voikin kadota matkalle. (Kaario 2002, 269–270.)

3.2.3 SNMP-viestit

SNMP:n toiminta on nimensä mukaisesti varsin yksinkertainen, jotta hallittavat laitteet selviävät helposti annetuista kyselyistä. Hallinta-asema ja agentti keskustelevat

keskenään ns. SNMP-viestien avulla. SNMPv1 sisältää viisi PDU-operaatiota (Protocol data unit) ja niiden lisäksi SNMPv2:n ja SNMPv3:n myötä lisättiin kolme uutta operaatiota. (Mauro & Schmidt 2005, 20.)

Kuviossa 1 on kuvattu yksinkertaisuudessaan hallinta-aseman (NMS) ja agentin välinen yhteys.



Kuvio 1. SNMP:n toiminta (Mauro & Schmidt 2005, 23)

GetReguest-tiedonkyselyoperaatiota käytetään, kun hallinta-agentilta halutaan lukea tietoja. Operaatiolla voidaan noutaa tietyn muuttujan tai muuttujien arvo agentilta. Halutut muuttujat on määritelty hallinta-asemassa. Kun kysely on tehty, agentti palauttaa vastauksen (*Response*) haluttujen muuttujien kanssa. (Mauro & Schmidt 2005, 66–69.)

SetReguest on puolestaan tiedonkirjoittamista varten. *Set*-operaatio on hyvin samanlainen kuin *Get*-operaatiokin, mutta sillä voidaan tehdä muutoksia haluttuihin muuttujiin. Operaatiota voidaankin käyttää esimerkiksi reitittimen asetuksien muuttamiseen. Vaikka *Set*-operaatiolla ei varsinaisesti voida tehdä suoraa käskyä esimerkiksi reitittimen uudelleenkäynnistyksestä, se voidaan kiertää asettamalla reitittimelle muuttuja sen tilasta, jonka voi *Set*-operaatiolla muuttaa tilaan 1 tai 0. (Mauro & Schmidt 2005, 76.)

GetNextRequest-operaatiolla pystytään kysymään kokonaisen MIB-ryhmän sisältö. MIB-kanta on puurakenteinen, ja kun *GeTNextRequest* suoritetaan, ajetaan komentoa *GetRequest* niin pitkään, että alipuun pääty on saavutettu. Taulusta haettavat rivit voidaan määrittää kyselyä tehdessä. (Mauro & Schmidt 2005, 69–70.)

GetBulkRequest lisättiin version SNMPv2 myötä ja se on optimoitu versio *GetNextRequestista*. Operaatiolla on mahdollista noutaa hallinta-asemalle suuria osia MBI-taulusta yhdellä haulla. Pelkällä *GetRequest*-kyselylläkin voidaan yrittää hakea enemmän, kuin yhtä muuttujaa kerralla, mutta agentin rajoituksista johtuen se ei välttämättä mene läpi. *Bulk*-operaatiota voidaankin käyttää pitkän *GetRequest* kyselyputken sijaan. *GetBulkRequest* pakottaa agentin lähettämään niin paljon tietoa kerralla, kuin mahdollista ja se mahdollistaa myös epätäydelliset vastaukset (toisin kuin *GetRequest*). Haun käyttäytymistä kontrolloidaan kentillä ”nonrepeaters” ja ”max-repetitions”. Näillä kentillä määritetään noudettavat objektit ja kuinka pitkään kyselyjä tehdään. (Mauro & Schmidt 2005, 74–75.)

Response on agentin lähettämä vastaus hallinta-asemalle, kun tietoja on kysytty. Hallinta-asemalle lähetetty viesti sisältää kysyttyjen MIB-objektien arvot, sekä mahdolliset virheilmoitukset. Kaikki edellä mainitut operaatiot johtavat lopulta agentin takaisin lähettämään *Response*-viestiin.

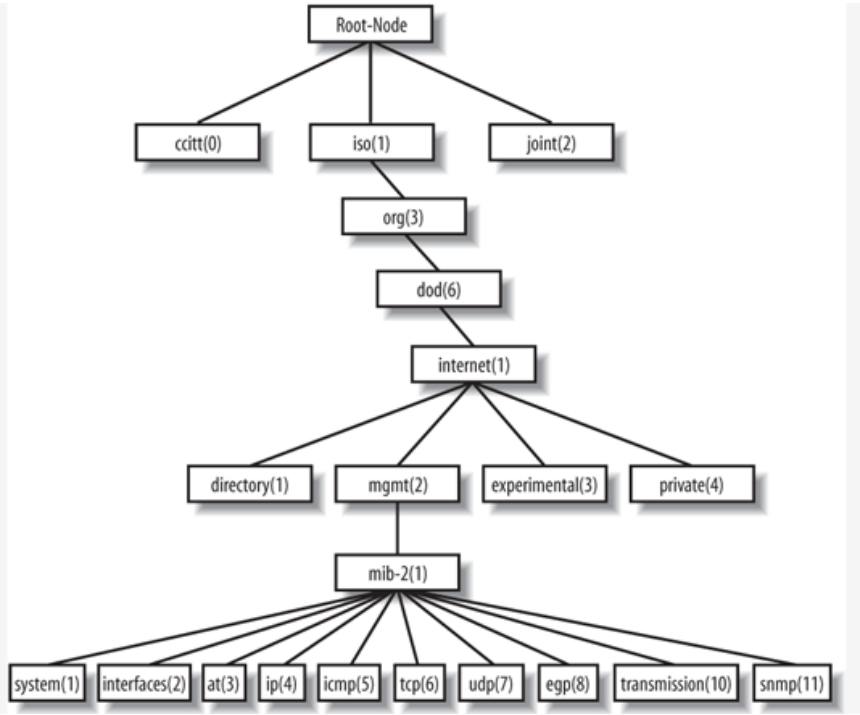
Trap on operaatio, jolla agentti voi lähettää omatoimisesti ilmoituksen hallinta-asemalle. SNMP-trap mahdollistaa agentin tiedottamaan hallinta-asemaa merkittävistä tapahtumista ilman erillistä pyyntöä hallinta-aseman toimesta. Lähetetty viesti on riippumaton hallinta-aseman tilasta, eikä vaadi kuittausta sen päästä. SNMPv2 sisältää uuden version Trapista ja se kulkeekin uudessa versiossa nimellä *SNMPv2-Trap.* (Mauro & Schmidt 2005, 80–81)

InformRequest tuli mukaan SNMPv2-version myötä. Tämä operaatio mahdollistaa hallinta-asemien välisen keskustelun ja tiedonvaihdon. Trap-viestin yksi heikkouksista on, ettei se tiedä onko lähetetty viesti ikinä mennyt perille kohdeasemalle. *InformRequest* mahdollistaa juuri tämän, eli se pystyy kuittaamaan viestit vastaanotetuiksi. Yksi käyttökohteista onkin Trap-viestien lähetys agentilta hallinta-asemalle, millä varmistetaan, että tieto hukatuista paketeista saadaan ylös. (Mauro & Schmidt 2005, 83)

Report otettiin käyttöön SNMP:n uusimmassa versiossa SNMPv3. Tällä operaatiolla mahdollistettiin SNMP-koneiden kommunikointi keskenään. Pääasiassa tätä operaatiota käytetään SNMP-viesteissä tapahtuvien virheiden prosessoinnissa. (Mauro & Schmidt 2005, 83)

3.3 MIB

SNMP:n tärkein hallintatietokanta on MIB-II, koska jokaisen laitteen, joka tukee SNMP:tä, tulee myös tukea MIB-II:sta (Mauro & Schmidt 2005, 63). MIB-II-tietokanta sisältää laitteen hallinnointiin tarvittavat tiedot muuttujina ja muuttujajoukkoina. Tämä SMI:n (Structure of Management Information) standardin mukaisesti määritelty tietokanta sisältää siis joukon objekteja (olioita), joista jokainen mittaa tiettyä arvoa hallittavasta laitteesta (esimerkiksi kytkimen muistikapasiteetti, MAC-osoite, vastaanotettujen pakettien määrä yms.). MIB:n hierarkkinen puumalli sisältää oman osoitteen jokaiselle objektille. Jokainen hallittava objekti tunnistetaan ASN.1–standardin (Abstract Syntax Notation One) määrittelemän ainutlaatuisen OID:n (Object Identifier) perusteella. OID kertoo objektin tarkan sijainnin MIB:n puurakenteisessa kannassa omana koodinaan. Esimerkiksi alapuu *System* on nimeltään 1.3.6.1.2.1.1. Hallinta-asema tekee omasta MIB-kannasta löytyvien objektien perusteella SNMP-kyselyn agentille, joka palauttaa halutun objektin, mikäli vastaava objekti löytyy agentin omasta kannasta. Kuviossa 2 on kuvattuna MIB-II-tietokannan puumaista rakennetta. (Kaario 2002, 274; Mauro & Schmidt 2005, 62–63.)



Kuvio 2. MIB-II puurakenne (Mauro & Schmidt 2005, 63)

3.4 RMON

Normaalien SNMP-standardien lisäksi on kehitetty etähallintastandardi RMON (Remote Network-Monitoring), jota pidetäänkin yleisesti tärkeimpänä lisäyksenä SNMP:n rinnalle. RMON määritellään RFC 1757 suosituksessa ja siitä uudistettu versio RMON2 suosituksessa RFC 2021. Tämä standardi täydentää MIB-II:ta ja sillä saadaan verkon tilasta kootusti tarkempaa dataa, kuormittamatta verkkoa yhtä paljon, kuin SNMP:n vastaavissa operaatioissa. SNMP-protokollaa käyttäessä verkko voi joutua huomattavan rasituksen kohteeksi ja tämän ongelman estämiseksi RMON kehitettiin. RMON:in avulla on mahdollistaa koko lähiverkon laitteiden seuraamisen huomattavasti pienemmällä rasituksella hallinta-asemille, agenteille ja verkolle, kuin SNMP. RMON-agentti (tämä tiedonkeruusyksikkö kulkee myös nimellä probe) asennetaan esimerkiksi valvottavaan reitittimeen, jonka kautta agentti kerää tietoa omaan MIB-tiedostoonsa, jota voidaan tutkia mikä ehkäisee verkossa esiintyvää

ruuhkaa verkkoa valvoessa. Toisaalta RMON on raskas sillä nimenomaisella koneella, johon sen agentti on kytketty johtuen suuren datamäärän analysoinnista. (Jaakohuhta 2002, 311–315; Kaario 2002, 279.)

3.5 ICMP

Ennen SNMP:n kehittämistä ei 1970-luvun lopullakaan ollut mitään oikeaa verkonhallintaprotokollaa. Työkalu, jota tuohon aikaan käytettiin, oli TCP/IP:n ICMP (Internet-Control Message Protocol). ICMP:n avulla voidaan lähettää viestejä reitittimistä ja tietokoneista muihin TCP/IP:tä käyttäviin laitteisiin. ICMP-viestien avulla voidaan selvittää laitteiden saatavuutta (onko laite ollenkaan päällä/vastaanottavassa tilassa) ja tutkia verkon viiveitä (latenssia). Tähän soveltuu parhaiten PING-ohjelma (Packet Internet Groper), jolla lähetetään ja vastaanotetaan ICMP-viestejä. ICMP on kaikkea muuta, kuin kuollut nykypäivänäkin. ICMP on edelleen kovassa käytössä sen yksinkertaisuuden ja keveyden vuoksi, eikä se myöskään vaadi erikseen juuri mitään oikeuksia, joten sen käyttäminen on todella helppoa ja vaivatonta. (Hautaniemi 1994, luku 4.1)

ICMP luotiin virhetilanteiden tiedon välittämiseen verkossa, eikä niinkään tekemään verkosta luotettavaa. Protokollatasolla se on heti IP:n yläpuolella, mutta se on periaatteessa osana IP-protokollaa, joten se löytyy kaikista IP-moduuleista. ICMP:n läheinen suhde IP:n kanssa onkin yksi syy ICMP:n yleisyyteen ja helppokäyttöisyyteen. Varsinaiset ICMP-sanomat kulkevat IP-sanoman sisällä ja sanomat sisältävät tyypin, koodin, tarkistussumman ja määrittelykentän muulle informaatiolle. (RFC792 1981, 1-4)

4. Qentinel NetEye

4.1 Ohjelmiston valinta

Ohjelmiston valintaan ei tässä työssä tarvinnut käyttää aikaa, koska toimeksiantajalla oli valmiina hankittuna verkkomonitorointiin tarkoitettu maksullinen Qentinel NetEye. Verkkomonitorointi sovelluksia on toki useita kymmeniä, ellei satoja, mutta tässä tapauksessa ”valinta” oli helppo ja NetEye sopii tämän verkkomonitorointityön tarpeisiin hyvin.

4.2 Yleistä

Qentinel NetEye on tarkoitettu valvomaan lähinnä yrityspuolen ICT-palveluita, verkkoa ja antamaan yleisnäkymän ICT-palvelun tuottamiseen liittyvien resurssien tilasta. Sovelluksen avulla saadaan aikaan hyvin kattava perusvalvonta, jonka osa-alueet voidaan jakaa loogisiin kokonaisuuksiin hyödyntäen sovelluksen ominaisuuksia.

Qentinel NetEye on selainpohjainen, eli kaikki hallinta ja valvonta suoritetaan web-käyttöliittymän kautta selaimella. Opinnäytetyön tekemisen hetkellä käytettiin NetEye-versiota 4.1.5 (Qentinel NetEye - Näkyvyyttä ICT-palveluihin. N.d.)

Tärkeimmät NetEyen ominaisuudet listattuna Qentinelin verkkosivuilta:

- Reaaliaikainen valvonta
- Skaalautuvuus erilaisiin ympäristöihin
- ICT-palvelujen visualisointi palvelukartoilla
- Helppokäyttöinen web-käyttöliittymä
- Käyttäjäryhmäkohtaiset näkymät
- Monipuoliset raportointiominaisuudet

- Käyttäjäsimulaatio
- Integroitavuus

(Qentinel NetEye - Näkyvyyttä ICT-palveluihin. N.d.)

4.3 Käyttöliittymä

4.3.1 Yleistä

Qentinel NetEyen käyttöliittymä on täysin web-pohjainen (http(s) protokolla). Käyttöliittymä on jaettu kahteen loogiseen ryhmään: monitorointi ja ylläpito. Ylläpidon puoli on tarkoitettu admin-oikeudet omaaville käyttäjille. Kaikki monitoroinnista saatu tieto sekä asetuksien konfigurointi voidaan erikseen määrittää halutuille ryhmille.

NetEyen päänäkymä on jatkuvasti päivittyvä sivu, joka näyttää halutun monitoroimalla saadun tiedon valituista kohteista. Sivu päivittyy automaattisesti tietyin väliajoin (voidaan itse määrittää) tai vaihtoehtoisesti, myös selaimella sivun päivittäminen onnistuu. Kuviossa 3 on esimerkki NetEye:n oletusnäkymästä (Main Display) välilehdeltä ”Service Latency”

Kuvio 3. Qentinel NetEye Main display / Service Latency

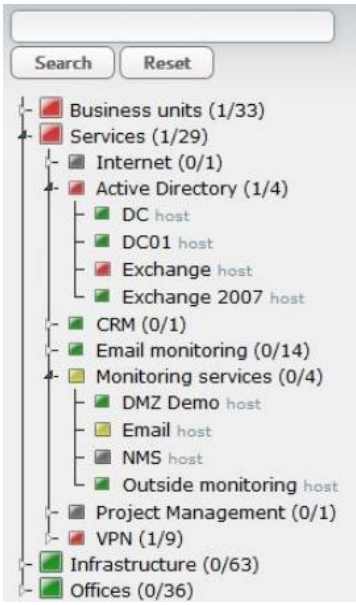
Käyttöliittymän päänäkymä koostuu kolmesta eri elementistä: profiilien puunäkymä (Profile Tree View), ylämonitorointinäkymä (Top Monitor View) ja ilmoitusnäkymä (Notification View). Näiden lisäksi ovat vielä omat näkymänsä kustomoitavalle reaaliaikaiselle näkymälle (Custom Real Time View), sähköpostin monitoroinnille (Email monitoring) ja tiedostoille (Files). (Qentinel NetEye 4.1.0 Administrator manual 2013, 7)

4.3.2 Puunäkymä

Päänäkymän vasemmassa reunassa sijaitsee profiilien puunäkymä. Puunäkymä on täysin kustomoitavissa, ja se voikin sisältää kaikkea SLA (Palvelutasosopimus eli Service Level Agreement) verifioinnin ja infrastruktuurinäkymän väliltä.

Jokaisen profiilin oikealla puolella on kaksi numeroa sulkujen sisässä. Oikeanpuoleinen luku kertoo isäntien (Host) kokonaismäärän kyseisen profiilin ja sen aliprofiilien

alla. Vasemmanpuoleinen luku kertoo puolestaan, kuinka moni isäntä on hälytystilassa kyseisen profiilin alla. Kuviossa 4 on esitettynä esimerkki puunäkymästä. Qentinel NetEye 4.1.0 Administrator manual 2013, 7-8).



Kuvio 4. Qentinel NetEye Puunäkymä

Kuviosta 4 nähdään, että profiileilla on tässä näkymässä olemassa 4 eri tilaa, jotka ovat kuvattuna erivärisinä neliöinä:

- Vihreä: Kaikki testit ovat menneet kyseiselle profiilille läpi.
- Keltainen: Varoitus tila, esimerkiksi joku isäntä ei vastaa SNMP kyselyyn.
- Punainen: Yksi tai useampi testi ei vastaa, tai testi on mennyt annetun rajaarvon yli ja on hälytystilassa
- Harmaa: Profiili toimintakyvytön ja sitä ei monitoroida, tai vaihtoehtoisesti yhtään isäntää ei ole aktiivisessa monitoroinnissa

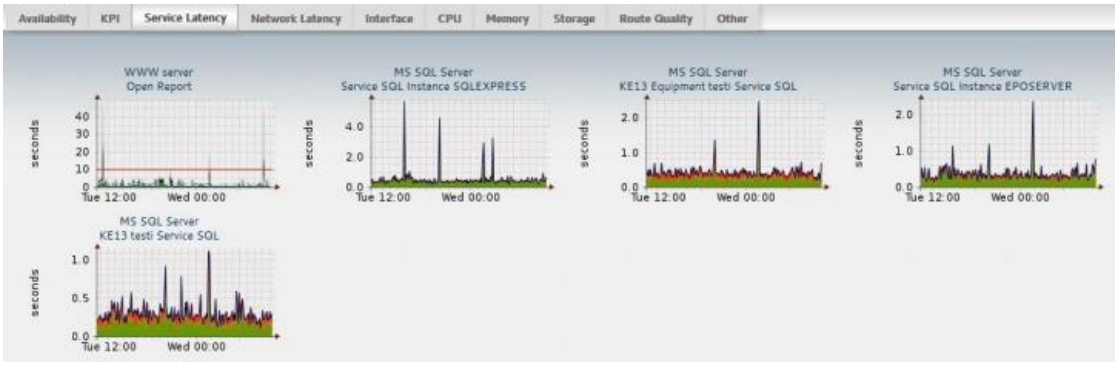
4.3.3 Monitoroinnin ylänäkymä

NetEyen päänäkymän yläreunassa sijaitsee monitoroinnin ylänäkymä. Kyseistä näkymää käytetään näyttämään aikaan perustuvia kuvaajia, jotka ovat jaettuina eri kategorioihin perustuen profiilille määritettyihin arvoihin. Jokainen NetEye objekti voidaan merkata KPI:ksi (Key Performance Indicator), millä objekti näkyy aina välilehden KPI alla. KPI-välilehden alle onkin tarkoitus laittaa yrityksen kannalta kaikkein kriittisimmät kaaviot. (Qentinel NetEye 4.1.0 Administrator manual 2013, 9-10)

Ylänäkymässä voi olla kaikkiaan 10 eri välilehteä. Välilehtien määrä riippuu järjestelmästä ja sille tehdyistä testeistä. Saatavilla olevat välilehdet NetEyen admin oppaassa lueteltuina:

- Availability
- KPI (Key Performance Indicators)
- Service Latency
- Network Latency
- Interface
- CPU
- Memory
- Storage
- Route Quality
- Other

Kuviossa 5 on esimerkki NetEyen ylänäkymästä



Kuvio 5. Qentinel NetEye Top Monitoring View

Jokaisesta kaaviosta voidaan avata yksityiskohtainen raportti-ikkuna klikkaamalla kaaviota. Tätä näkymää voi mukauttaa ja halutut kaaviot voidaan tallentaa PDF, PNG tai SVG tiedostoiksi.

4.3.4 Ilmoitusnäkymä

Päänäkymän alareunassa on Ilmoitusnäkymä, jonka tarkoituksena on näyttää kaikki hälytykset ja tapahtumat, mitkä koskevat valittua monitoroitavaa ympäristöä. Ilmoitusnäkymässä on 4 eri välilehteä: Hälytykset (Alerts), Tapahtumat (Events), Lokit (Logs) ja Trapit (Traps).

Alerts välilehti näyttää kaikki hälytykset ja varoitukset, jotka järjestelmä generoi monitorointi tapahtumista. Yleisin hälytyksen/varoituksen aiheuttaja on, kun mitattavan arvon raja-arvo ylittyy, laite ei vastaa tai monitoroitu sisältö sisältää virheitä. Kuviossa 6 on kuvattu esimerkki ”Alerts” välilehdestä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 10–11)

Kuvio 6. Qentinel NetEye Alerts välilehti

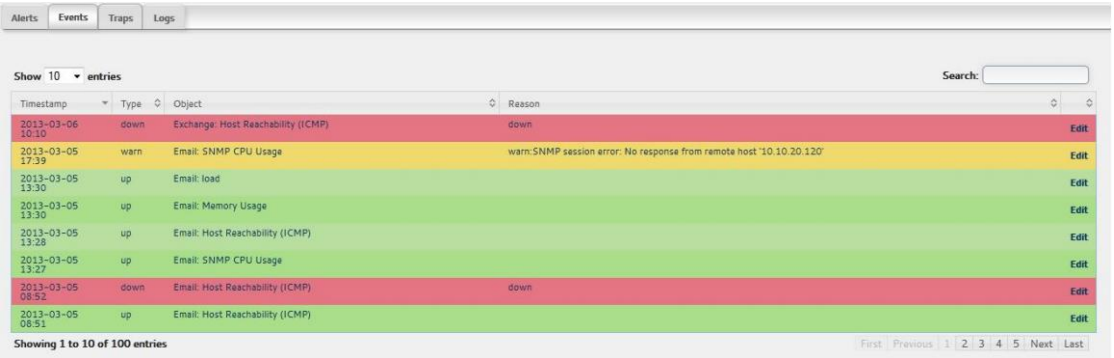
Yllä olevasta kuvasta nähdään, että myös hälytykset ovat kuvattu värikoodein. Punainen ja keltainen taustaväri kertoo parhaillaan meneillään olevista tapahtumista ja vihreä kertoo tapahtumahistorian.

- Punainen tausta: Hälytys – Monitoroidun objektin katsotaan olevan alhaalla. Mitattu arvo in ylittänyt määritetyn raja-arvon tai laitteeseen ei saada yhteyttä. Duration sarakkeesta nähdään, kuinka kauan tilanne on ollut päällä.

- Keltainen tausta: Varoitus – Tehty testi on varoitus-tilassa. Esimerkiksi monitoroitava isäntä ei vastaa SNMP-viesteihin tai varoitus raja-arvo on ylittynyt.

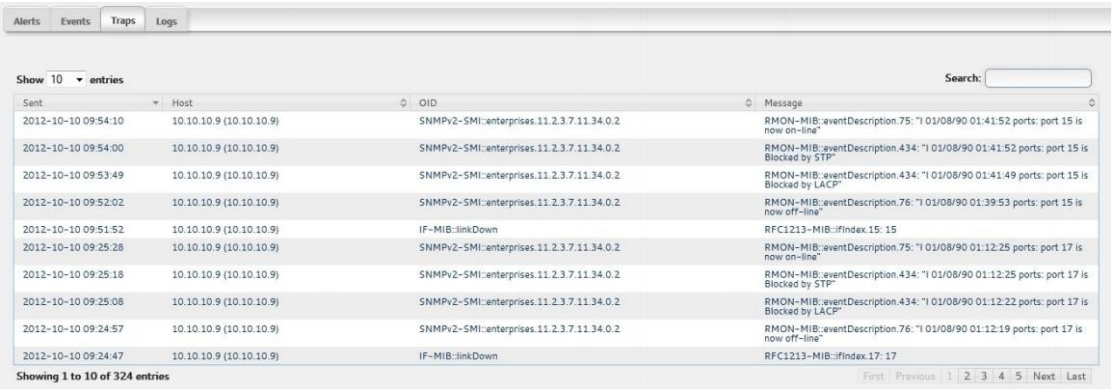
- Vihreä tausta: Hälytys tai varoitus tapahtumahistoria – Mitattu arvo on ollut hälytys/varoitus tilassa, mutta on alkanut jälleen vastaamaan. Aloitus ja lopetusajat nähdään sarakkeista ”start” ja ”end”.

Events välilehti näyttää kaikki tapahtumat, jotka ilmenevät monitoroitavassa järjestelmässä kumulatiivisessa järjestyksessä. Tapahtumat voivat vaihdella epäonnistuneista testeistä järjestelmän lähettämiin viesteihin ja joitain näistä tapahtumista käytetäänkin hälytysten luontiin Hälytys välilehdelle. Kuviossa 7 nähdään esimerkki Tapahtumat välilehdestä. Värikoodit ovat jälleen samat, kuin aiemmin. (Qentinel NetEye 4.1.0 Administrator manual 2013, 12)



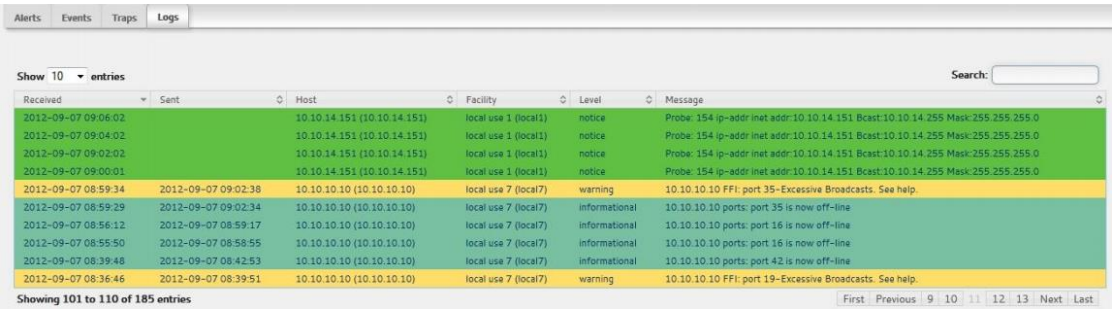
Kuvio 7. Qentinel NetEye Events välilehti

Traps välilehti näyttää kaikki SNMP-trap viestit, jotka ovat määritetty vastaanotettaviksi. Välilehdellä näkyy milloin trap on lähetetty, viestin alkuperä, OID-tieto, sekä itse viestin arvot. Kuviossa 8 nähdään esimerkki Traps välilehdestä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 12)



Kuvio 8. Qentinel NetEye Traps välilehti

Logs välilehti näyttää järjestelmälokin (syslog) viestit, jotka Qentinel NetEyen *Syslog* testi on konfiguroitu vastaanottamaan. Valittu vakavuusaste ja järjestelmälokin testien kategoria vaikuttavat siihen, mitkä viestit näkyvät tällä välilehdellä. Logs välilehden viestit ovat jaettu seuraaviin kategorioihin: emergency (hätätila), alert (hälytys), critical (kriittinen), error (virhe), warning (varoitus), notice (huomio), info ja debug. Kuviossa 9 on esimerkki Logs välilehdestä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 13).



Kuvio 9. Qentinel NetEye Logs välilehti

4.3.5 Custom Real Time View

Custom Real Time View ikkunaan pääsee käsiksi päänäkymän oikeasta yläkulmasta. Tämän ominaisuuden avulla voidaan luoda kustomoitu näkymä, joka voi olla avuksi, jos halutaan tarkastella esimerkiksi isäntiä eri profiileiden alta. Näin saadaan tiivistettyä esimerkiksi toimipisteen kriittisimmät palvelut kätevästi yhteen paikkaan. (Qentinel NetEye 4.1.0 Administrator manual 2013, 13)

4.3.6 Sähköpostin monitorointi

Sähköpostin monitoroinnilla tarkastellaan, kulkevatko sähköpostit molempiin suuntiin mallikkaasti. Uloslähtevän sähköpostin toimivuutta tarkastellaan lähettämällä viesti paikallisen postipalvelimen kautta ulkoisen operaattorin postilaatikkoon. Saapuvien viestien toiminta testataan puolestaan lähettämällä operaattorin SMTP palvelimelta viesti paikalliseen postilaatikkoon. Testi katsoo kulkevatko viestit ja millä viiveellä ne liikkuvat. Myös viruksien ja roskapostin tarkistamiseen voidaan konfiguroida omat filtterinsä. Hälytys generoituu, mikäli posti ei liiku ajallaan tai viesti jää virus/roskaposti tarkistukseen. Kuviossa 10 on esimerkki sähköpostin monitoroinnin näkymästä. (Qentinel NetEye 4.1.0 Administrator manual 2013, 14)

Kuvio 10. Qentinel NetEye Email Monitoring

5. Suunnittelu

5.1 Yleistä

Tässä luvussa käydään läpi käytännön toteutuksen suunnittelua ja sen vaatimuksia. Valvonnan toteutusta suunniteltiin toimeksiantajan kanssa yhteistyössä ja ideoita tuli lisää työn edetessä.

Tehtävänä oli yksinkertaisuudessaan ottaa käyttöön verkonvalvonta ohjelmisto Qentinel NetEye ja lisätä sen valvonnan piiriin halutut laitteet halutuilla kriteereillä. Tässä ”ensimmäisen vaiheen” valvonnassa tarkoituksena oli ennen kaikkea saada kasaan

paketti, jolla pystytään tarkastelemaan, että Baronan – ja ennen kaikkea Puolan palvelukeskuksen – kriittisimmät palvelut ja tietoverkkoliikenne ovat toiminnassa ongelmitta. Myöhemmin valvontaa voidaan lisätä, mikäli se nähdään tarpeelliseksi.

5.2 Suunnittelu

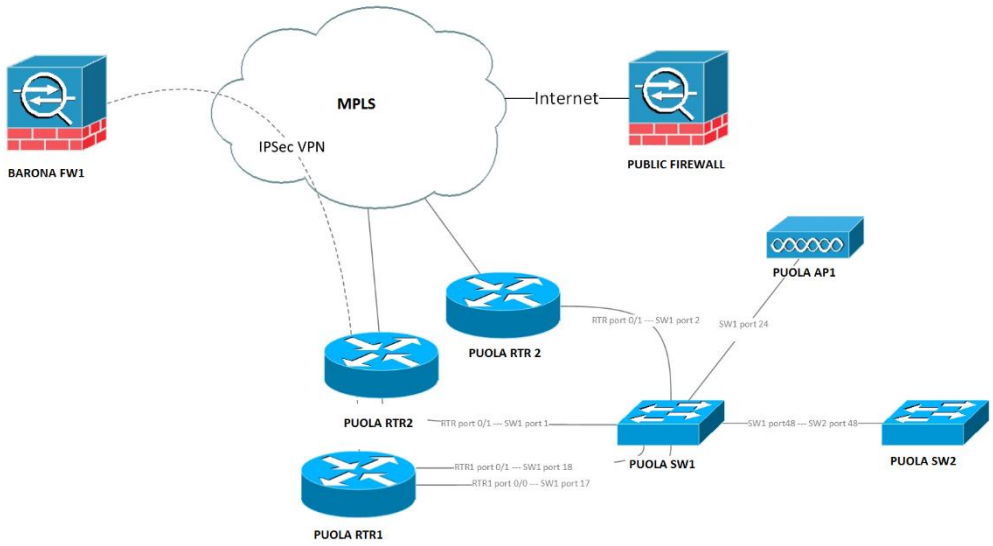
Monitoroinnin toteutuksen kanssa toimeksiantajan toiveena oli saada valvonnan alle elementtejä, jotka ovat kaikkein kriittisimpiä palvelukeskuksien toimintojen takaamiseksi. Tehtävänä oli saada kasaan rajattu joukko valvottavia laitteita, joilla kuitenkin saadaan hyvä käsitys palvelukeskuksien tilasta ja pystytään mahdollisten vikatilanteiden jälkeen tutkimaan, mikä on mennyt pieleen. Valvottaviin laitteisiin tulisi kuulumaan kytkimiä, reitittimiä tai palomuureja, sekä muutamia kriittisiä palvelimia. Näiden lisäksi kaikkein kriittisimpien tietoverkkoon liittyvien hälytyksien osalta, tulisi lähteä tieto asianomaisille, jotta suuremmat ongelmat saadaan varmasti selvitykseen mahdollisimman nopeasti.

Valvonnan alle haluttiin saada, myös tiettyjen verkkorajapintojen läpi kulkevan liikenteen määrä. Liikenteen määrää tutkimalla saataisiin toimeksiantajalle arvokasta tietoa, jonka avulla voitaisiin tutkia esimerkiksi mahdollisia piikkejä tietoliikenteessä ja tätä kautta edelleen löytää potentiaalisia pullonkauloja ja auttaa ongelmatilanteiden selvityksessä.

NetEyen perusnäkymästä tulee myös saada looginen ja helppokäyttöinen. Heti sovellusta avattaessa tulee käydä ilmi, onko valvonnan alla olevissa laitteissa akuutteja hälytyksiä päällä. Kriittisimmistä hälytyksistä tulee myös lähettää sähköposti- tai SMS-viesti asianomaisille tahoille.

5.3 Verkkokuva

Suurin osa valvonnasta tulee siis keskittymään Puolan palvelukeskuksen toimintaan, mutta muutamia muita Puolan ulkopuolisiakin laitteita tulee valvonnan alle. Kaikki Puolasta lähtevä liikenne kulkee Suomen kautta, joten tietoverkkoihin liittyvät ongelmat voivat hyvinkin johtua myös Suomen päästä. Myöskään valvottavat palvelimet eivät ole fyysisesti Puolassa, mutta ne ovat silti toiminnan kannalta kriittisiä, sillä nämä palvelimet ovat Katowicen palveluskeskuksessa jatkuvassa käytössä. Kuviossa 11 on käyty läpi Katowicen palvelukeskuksen verkkotopologiaa.



Kuvio 11. Katowicen palvelukeskuksen verkkokuva

5.4 Valvottavien laitteiden valinta

Valvottavat laitteet tuli valita siten, että kaikkia kriittisimpiä palveluita voidaan tarkkailla ja varmistaa tietoverkon toimivuus, mutta samalla kuitenkin pitää valvottavien laitteiden määrä suhteellisen pienenä. Ei ollut tarkoituksenmukaista ottaa valvontaan

jokaista mahdollista laitetta jokaiselta toimipisteeltä, sillä esimerkiksi tietoverkon toimivuuden varmistamiseksi riittää muutamien avainasemassa olevien laitteiden valvonta.

Esimerkkinä ylempänä olevan verkkokuvan perusteella voidaan katsoa, että Katowicen palvelukeskuksen kaikki liikenne kulkee SW1:en kautta, joten tämä kytkin laitetaan ehdottomasti valvonnan alaiseksi. Jos kyseinen kytkin on pois toiminnasta, niin voidaan olla varmoja, että koko palvelukeskuksen verkkoyhteydet ovat ongelmissa. Toinen todella tärkeä osa kyseisestä verkkokuvasta on vasemmalta ylhäältä löytyvä palomuuri ”BARONA FW1”, sillä kyseinen palomuuri on Suomen päässä ja Katowicen liikenne kulkee sen kautta Suomeen.

Lopulta toimeksiantajan kanssa päädyttiin laittamaan valvonnan alle 5 palvelinta ja 5 laitetta tarkkailemaan tietoverkkojen tilaa. Taulukossa 1 on listattu kaikki valvontaan asetetut laitteet ja niissä käytetyt mittarit.

Taulukko 1. Valvottavat laitteet

Valvottava laite	Käytetyt mittarit	Raja-arvo
Kytkin SW1	Saatavuus Yhteyden Laatu Liikenteen määrä (Interface)	- 25 % pakettihävikki 90 %
Kytkin SW10	Saatavuus Yhteyden laatu Liikenteen määrä (Interface)	 25 % pakettihävikki 90 %
Kytkin SW20	Saatavuus Yhteyden laatu	- 25 % pakettihävikki
Reititin RTR1	Saatavuus Yhteyden laatu	- 25 % pakettihävikki
Palomuuri FW1	Saatavuus Yhteyden laatu	- 25 % pakettihävikki
Palvelin P1	Saatavuus CPU:n Käyttöaste Muistin käyttöaste	- 90 % 90 %
Palvelin P2	Saatavuus CPU:n käyttöaste Muistin käyttöaste Palvelut	- 90 % 90 % -
Palvelin P3	Saatavuus CPU:n käyttöaste Muistin käyttöaste Palvelut	- 90 % 90 % -
Palvelin P4	Saatavuus CPU:n käyttöaste Muistin käyttöaste Palvelut	- 90 % 90 % -
Palvelin P5	Saatavuus CPU:n käyttöaste Muistin käyttöaste Palvelut	- 90 % 90 % -

5.5 SNMP-versio

Käytettävän SNMP-version valintaan ei tarvinnut käyttää paljon aikaa sillä työssä käytetyn NetEyen versio tukee SNMP:tä versio SNMPv2c:hen asti, joten jokainen SNMP-valvonnan piiriin lisätty laite tulikin lopulta käyttämään juuri tuota kyseistä versiota. Itse verkkolaitteisiin ja palvelimiin ei opinnäytetyötä tehdessä ollut pääsyä, joten niihin ei voinut mennä SNMP:tä konfiguroimaan. SNMP-konfigurointi hoituikin kolmannen osapuolen toimesta ja esimerkiksi SNMP:n käyttöönottoon tarvittavat ”yhteisönimet” (Community string) tulivat tätä kautta.

6. Toteutus

6.1 Yleistä

Toteutus-vaiheessa tavoitteena oli saada valitut laitteet monitoroinnin alaiseksi käyttäen Qentinelin maksullista NetEye ohjelmaa. NetEye tuli myös konfiguroida tarpeiden ja vaatimuksien mukaisesti, päällimmäisen tavoitteen ollessa helppokäyttöisyys ja selkeys. Tässä kappaleessa käydään läpi vaihe vaiheelta verkkomonitoroinnin toteutuksen käytännön toimenpiteet, sekä tutustutaan tarkemmin valvonnan alle asetettuihin laitteisiin.

6.2 Yleisnäkymän konfigurointi

Qentinel NetEyen ”etusivulle” tulee määritellä halutun kaltainen puunäkymä. Tästä puunäkymästä voidaan heti nähdä, onko kyseisen puunäkymän oksien alla hälytyksiä sillä kyseisellä hetkellä. Toimeksiantajan kanssa päädyttiin siihen lopputulokseen,

että valvottavat laitteet luokiteltiin kahteen eri haaraan aktiivisen valvonnan alle: ”Tietoliikenne” ja ”Palvelimet”. Tähän luokitteluun päädyttiin, koska todettiin, että tietoverkkojen hälytykset ovat kriittisemmässä roolissa, kuin palvelimien vastaavat. Tällä luokittelulla voidaan heti katsoa, että hälytykset tulevat nimenomaan tietoverkoista, eivätkä palvelimet ole välissä aiheuttamassa hälytyksiä. Toinen vaihtoehto luokittelulle olisi ollut esimerkiksi toimipisteiden mukainen lajittelu, mutta se katsottiin tässä tapauksessa tarpeettomaksi.

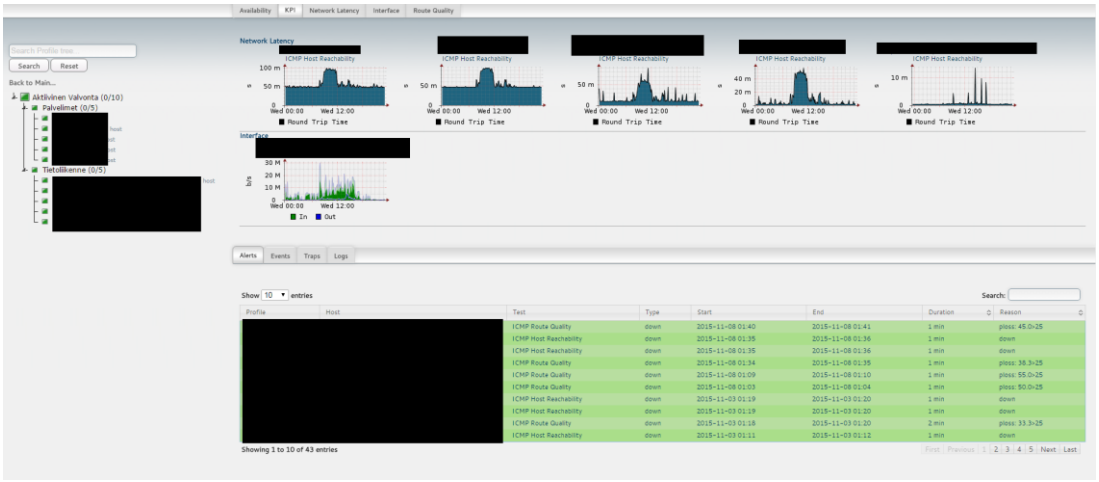
Käytännössä lopulliseen näkymään tuli puuhun kaksi oksaa, joiden alle lisättiin kaikki valvottavat laitteet oman oksansa alle. Sekä Palvelimet- että Tietoliikenne-välilehden alle tuli molempiin viisi laitetta.

Puunäkymän lisäksi NetEyen aloitusnäkymään voi määrittää KPI-mittarit. Tähän KPI-näkymään voi määrittää minkä tahansa valvotun laitteen kyselyn. Toisin sanoen KPI-näkymään kannattaa lisätä kriittisimmät valvonnan kohteet, että ne ovat helposti näkyvillä. Tässä verkkomonitoroinnin toteutuksessa laitettiin jokaisesta eri toimipisteillä sijaitsevista tietoliikennelaitteesta saatavuuskysely KPI-näkymään. Saatavuus-kyselyllä tarkoitetaan siis Host Reachability ICMP-kyselyä, eli käytönnössä valvottavaan laitteeseen lähetään ping-kutsu, jonka avulla varmistetaan kyseisen laitteen saatavuus. Kyseisen kutsun avulla saadaankin nopeasti selville valvottavien laitteiden saatavuuden lisäksi viive (eli latenssi). Jokaiselta toimipisteeltä lisättiin ainakin yksi solmukohdan tietoverkkolaite, jotta toimipisteiden tietoverkon tilannetta olisi helppo seurata yhdellä silmäyksellä.

Päänäkymä on aloitussivun lisäksi pohja kaikille muille alisivuille. Esimerkiksi puunäkymästä voidaan valita tietty haara, minkä jälkeen vastaavanlainen näkymä näyttää samat kategoriat, mutta ne koskevat vain sen kyseisen haaran laitteita. Toisin sanoen näkymällä voidaan katsoa vaikka sadan eri laitteen tilannetta kerralla, tai vaihtoehtoisesti tutkia vain yhden laitteen kuvaajia.

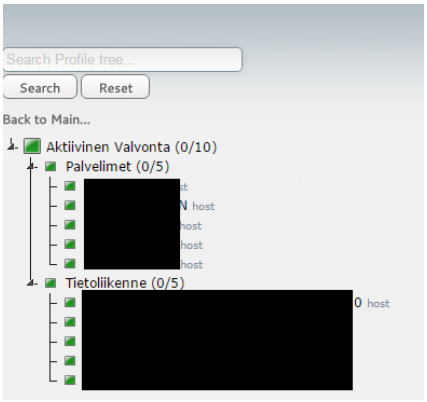
Kuviossa 12 - 15 on kuvattuna työn lopullinen päänäkymä. Vasemmalla on profiilin puunäkymä, johon on siis sijoiteltuna yllä mainitut laitteet palvelimien ja tietoliiken-

teen oksiin. Keskellä sivua näkyy viiden eri laitteen saatavuus-kyselyn tilanne edellisen 24 tunnin ajalta sekä yksi verkkorajapintakysely, josta nähdään edellisen 24 tunnin liikenteen määrä valitun kytkimen verkkorajapinnasta. Viimeisenä sivun alalaidassa on auki oletuksena ”Alerts”-välilehti, jossa nähdään oletuksena 10 viimeisintä aktiivista/tapahtunutta hälytystä. KPI- ja Alerts-välilehteä voidaan vaihtaa kuvioissa näkyviin eri vaihtoehtoihin, jotka näyttävät kyseiselle valinnalle rajatun näkymän. Kuviossa 12 on kuvattuna koko loppukäyttäjälle näkyvä päänäkymä.



Kuvio 12. Lopullinen päänäkymä kokonaisuudessaan

Kuviossa 13 on kuvattuna lopullisen valvonnan puunäkymä. Kuvasta nähdään oksat ”Palvelimet” ja ”Tietoliikenne”, joiden alle on lajiteltuna valvottavat laitteet. Tässä kuvan tapauksessa kaikki on kunnossa, sillä jokainen symboli on vihreänä, ja ”Aktiivinen valvonta” kertoo hälytyksien/varoituksien määräksi 0/10 (ks. luku 4.3.1).



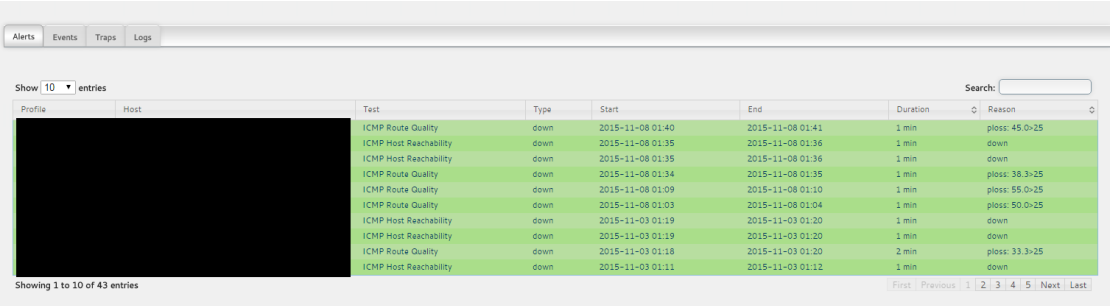
Kuvio 13. Lopullinen päänäkymä: profiilin puunäkymä

Kuvio 14 näyttää puolestaan KPI-välilehden sisällön. KPI-välilehti on oletuksena aina auki oleva tietosivu, jossa näkyvät kuvaajat ovat itse määriteltävissä. Tässä työssä kyseiselle välilehdelle päädyttiin laittamaan ICMP-kyselyt, sekä palvelimien, että tietoliikenteen puolelta. Tämän lisäksi, myös yhden tärkeän kytkimen verkkorajapintakaavio asetettiin näkymään tietoliikenne-oksan KPI-välilehdelle. Näillä tiedoilla pystytään nopeasti katsomaan, onko edellisen 24-tunnin aikana tapahtunut jotain huomioitavaa.

Kuvio 14. Lopullinen päänäkymä: KPI-välilehti

Päänäkymän alareunassa on oletuksena auki Alerts-välilehti, josta nähdään päällä olevat hälytykset/varoitukset, sekä ohimenneet tapahtumat. Vihreällä pohjalla merkityt tapahtumat ovat vanhoja hälytyksiä ja tästä näkymästä voidaan katsoa miksi hälytys on syntynyt, milloin se on ilmennyt ja kuinka kauan se on kestänyt. Punainen ja

keltainen väri puolestaan kertoisi, että hälytys on vieläkin ajankohtainen. Seuraavassa kuviossa on esitettynä tämä Alerts-välilehti. Kuviosta 15 nähdään, että kyseisellä hetkellä ei ole hälytyksiä päällä, mutta edellisen viikon aikana tapahtumia on kuitenkin ollut.

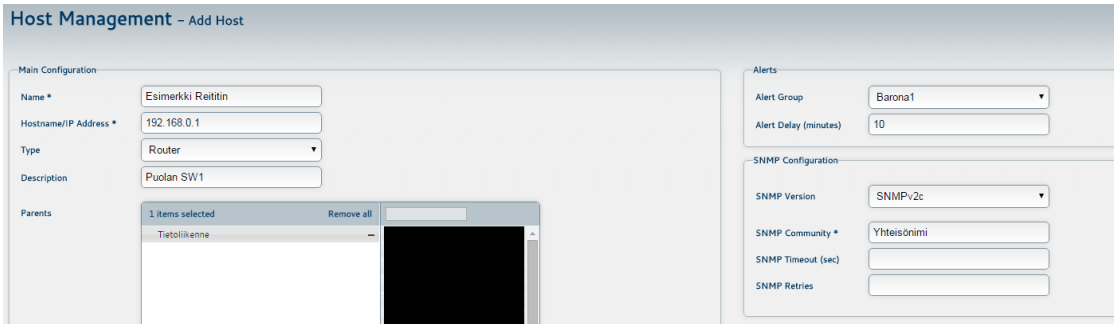


Kuvio 15. Lopullinen päänäkymä: Hälytykset-välilehti

6.3 Laitteiden lisäys NetEyessa

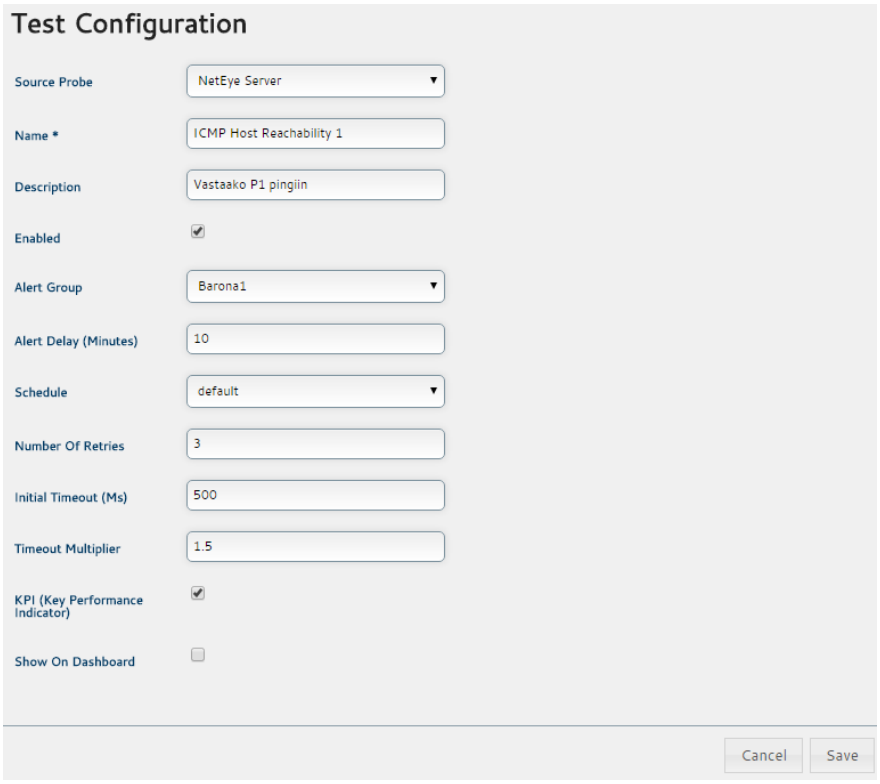
Varsinainen laitteiden lisäys NetEyen profiilien alle oli varsin yksinkertainen prosessi, kunhan valvottava laite oli päätetty ja oli selvää, mitä siitä halutaan valvoa. Valvottavasta laitteesta tulee tietää vain sen IP-osoite, mikä laite ylipäätänsä on (reititin, palvelin, kytkin yms.) ja sen SNMP:n yhteisönimi. Kun nämä tiedot ovat selvillä, on laitteiden lisääminen mekaanista tekemistä NetEyen käyttöliittymän avulla. Pudotusvalikosta voidaan valita haluttu kysely kaikkien saatavilla olevien vaihtoehtojen joukosta, ja valinnan mukaan säätää esimerkiksi hälytyksien raja-arvoja mieleiseksi.

Kuviossa 16. näkyy esimerkki ”Add Host”-sivusta. Kuvasta nähdään vaaditut kentät ja jo tässä vaiheessa voidaan määrittää, jos kaikista hälytyksistä halutaan käyttää tiettyä ennalta määrättyä ryhmää (Alert Group).



Kuvio 16. Add Host-sivu

Kun laitteet ovat lisättyinä NetEyen käyttöliittymään, tulee seuraavaksi lisätä testit, joita laitteelle halutaan ajaa. Tämä tapahtuu lisäämällä aktiivisen valvonnan piiriin pudotusvalikosta haluttu testi, ja konfiguroimalla sille tarvittavat arvot, sekä asetukset. Säädettäviä asetuksia ovat esimerkiksi hälytysryhmät, kuinka usein testiä ajetaan tai halutaanko testi KPI-näkymään. Kuviossa 17 on esimerkki ”ICMP Host Reachability”-testin konfigurointisivusta.



Kuvio 17. Testin Konfiguraatiosivu

6.4 Tietoliikennelaitteiden lisäys

Kuten aiemmin jo mainittiin, niin lopulta tietoverkkolaitteiden puolelta päädyttiin lisäämään kokonaisuudessaan viisi eri laitetta valvottavaksi. Tavoitteena oli saada hyvä kuva eri toimipisteiden verkkojen tiloista ja lisäksi saada haluttujen porttien läpikulkevasta liikenteestä dataa. Näiden vaatimuksien perusteella valvottaviksi hallinta-agenteiksi valittiin kolme eri kytkintä, yksi reititin ja yks palomuuri. Nämä laitteet sijaitsevat fyysisesti kolmessa eri sijainnissa ja niitä valvomalla saadaan hyvä yleiskäsitys varsinkin Puolan toimipisteen verkkoyhteyksien toimivuudesta.

Käytännössä jokaisesta laitteesta laitettiin ICMP:n saatavuus- ja laatukysely monitorointiin, minkä avulla pystytään tarkkailemaan ovatko laitteet ylipäätänsä pystyssä ja onko latenssi tai pakettihävikki huolestuttavalla tasolla. Nämä ICMP-kutsut olivatkin tämän verkkomonitoroinnin toteutuksen kannalta kaikkein tärkeimmät kyselyt. Etenkin Puolan palvelukeskuksen kannalta haluttiin saada verkkolaitteista tarkkaa tietoa, että mahdolliset ongelmat saadaan heti havaittua, sekä pienempiä häiriöitä voidaan jälkikäteen tutkia tulevien ongelmien ehkäisemiseksi.

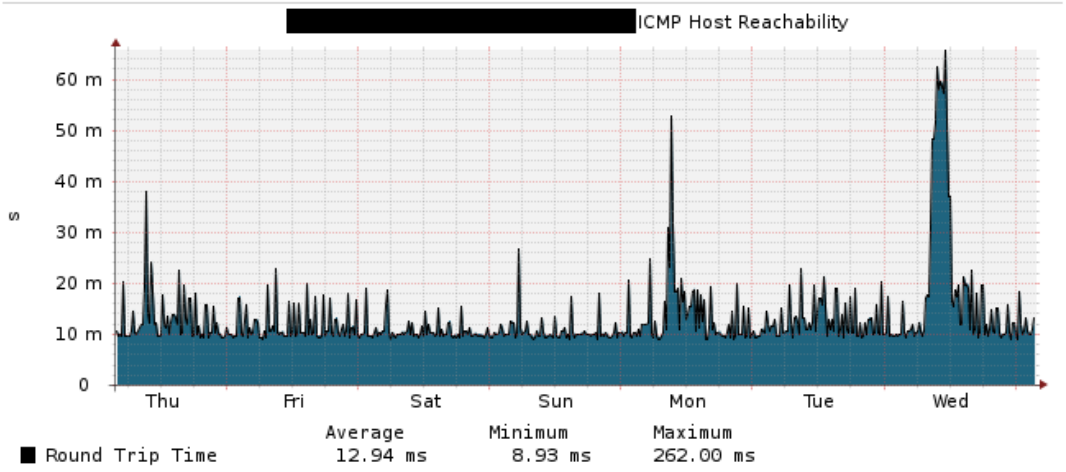
Toinen tärkeä kysely, jota työssä käytettiin oli SNMP:n Interface-, eli verkkorajapintatesti. Tällä kyselyllä valvottavasta laitteesta saadaan tieto tietyn verkkorajapinnan läpi kulkevan liikenteen määrästä. Tätä tietoa voidaan käyttää hyväksi kun, esimerkiksi halutaan analysoida tuleeko tiettyinä kellonaikoina isoja piikkejä tietoliikenteeseen tai rasittaako esimerkiksi julkinen WLAN liikaa tietoverkkoa. Verkkorajapintatesti laitettiin tässä työssä kahteen eri kytkimeen, joista toinen on nimenomaan Puolan toimipisteessä.

6.4.1 ICMP Testit

ICMP-testeillä pystytään siis tutkimaan laitteiden saatavuutta ja yhteyden laatua ICMP-pakettien avulla. Jokaiselle viidelle valitulle tietoverkkolaitteelle laitettiin nämä

ICMP-kyselyt ja näistä kyselyistä piirtyy kuvaajia sitä mukaa, kun tietoa liikkuu. Kuvaajia voidaan NetEyen avulla tutkia niin pitkältä ajalta, kuin halutaan ja kuvaajat voidaan tallentaa NetEyen kautta suoraan esimerkiksi PDF-muotoon.

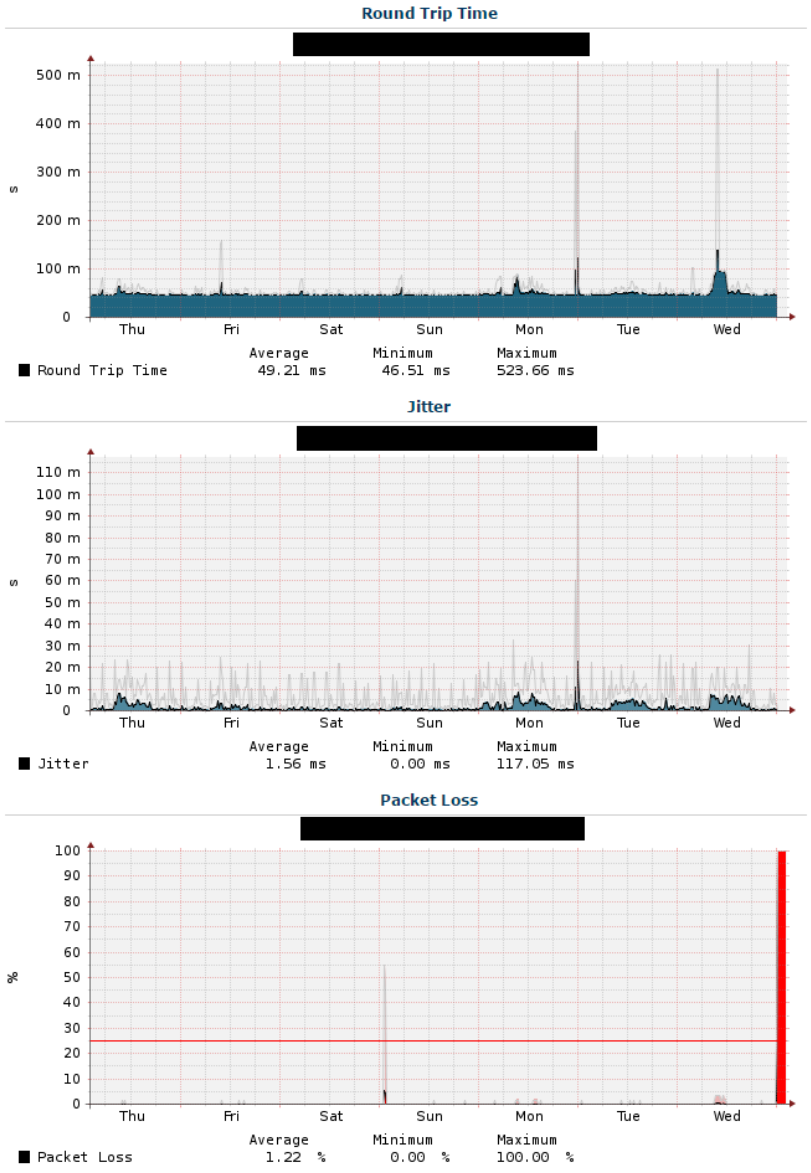
ICMP-Reachability – eli saatavuus-testi – on tämän opinnäytetyön kannalta kaikkein tärkein käytetty työkalu. Saatavuuden tarkastelulla tutkitaan nimensä mukaisesti halutun laitteen saatavuutta, eli sitä, onko laite online-tilassa ja käytettävissä. Käytännössä NetEye lähettää tietyn määrän ”ICMP echo”-kyselyjä hallinta-agentille ja odottaa vastausta. Jos yksikään paketti ei tule takaisin, katsotaan agentin olevan saavuttamattomissa ja tästä tapahtumasta luodaan hälytys. Ja koska tähän kyselyyn tulee vain kaksi vastausta: ”up” tai ”down”, niin hälytykselle ei tarvitse asettaa erikseen mitään raja-arvoa. Kyselyn sivutuotteena saadaan myös aika, joka paketilta kuluu matkaan lähettäjältä vastaanottajalle, eli latenssi. Kuviossa 18 on erään kytkimen viikon ajalta piirtynyt kuvaaja käyttäen saatavuus-kyselyä. Kuvaajasta nähdään itse käyrän lisäksi lukemat keskiarvosta, minimistä ja maksimista.



Kuvio 18. Route Reachability

ICMP-Route Quality-testillä saadaan valvottavasta laitteesta selville Latenssi (Round Trip Time), viiveen vaihtelu (Jitter eli huojunta), sekä pakettihävikki (Packet Loss). Periaate on tällä testillä täysin sama, kuin saatavuuskyselyllä, mutta NetEye palauttaa

tällä hieman enemmän tietoa, kuin pelkkä saatavuus-kysely. Kuviossa 19 on esimerkki erään laitteen Route Quality-sivusta yhden viikon ajalta.



Kuvio 19. Route Quality-testi

Kuviosta 19 nähdään, että kuvaajien lisäksi saadaan tieto keskiarvoista, minimeistä ja maksimeista. Tässä esimerkissä pystytään lisäksi havaitsemaan, että kyseisen laitteen pakettihävikki on kuvaajan loppupäässä 100 %, ja latenssista, eikä viiveen vaihtelusta dataa ole saatavilla ollenkaan. Tästä voidaan päätellä, että kyseinen laite on tuolloin

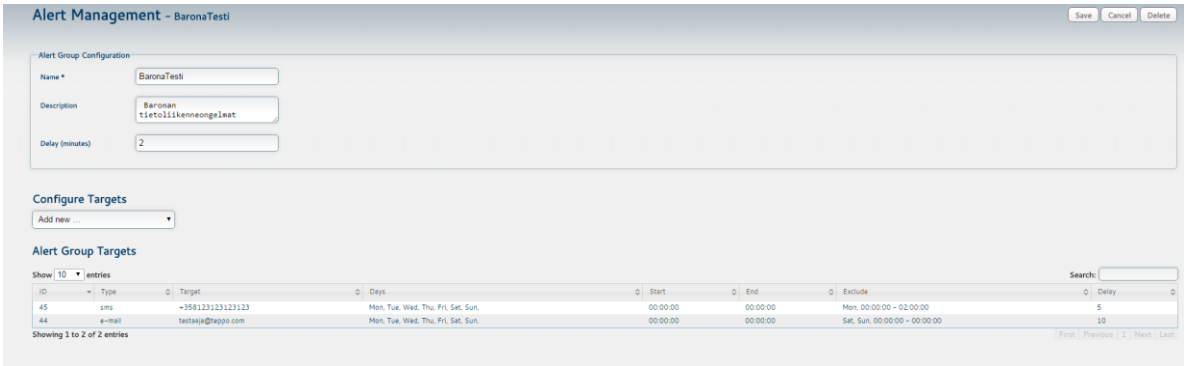
ollut kokonaan alhaalla. Pakettihäviön kuvaajassa nähdään, myös punainen poikkiviiva, joka kuvaa hälytyksen raja-arvoa. Pakettihäviön kohdalla jokaiselle laitteelle annettiin hälytyksen raja-arvoksi 25 %. Pakettihäviön tulisi toki olla lähes nollassa koko ajan, mutta katsottiin, että 25 prosentin kohdalla alkaa hävikki olemaan tietoliikenteen kannalta aivan liian suuri, joten tämän rajan ylittyessä siitä muodostuu hälytys NetEyelle. Latenssin ja jitterin kohdalla hälytysarvoja - ainakaan tässä vaiheessa – ei nähty tarpeellisiksi asettaa. Latenssin tai jitterin hetkittäinen nousu harvemmin on kriittinen ongelma ja tällaisten ongelmien ilmetessä se yleensä nähdään, myös laitteen saatavuuden tai pakettihävikin puolella. Kuvaajista voidaan toki myöhemmin tarkastella näitä ongelmakohtia, jos se nähdään tarpeelliseksi.

6.4.2 Hälytykset

Kaikki hälytykset tulevat siis näkyviin NetEyen käyttöliittymään ja tämä koskee tietenkin myös ICMP-hälytyksiä. Hälytykset tulevat näkyviin Alerts-välilehdelle, josta myös vanhempia, ja jo ohi menneitä hälytyksiä voi tutkia. Tämän lisäksi NetEyen avulla on mahdollista tehdä jatkotoimenpiteitä hälytyksien suhteen. Aiemmin mainittiinkin, että hälytyksistä voidaan lähettää tieto ylläpitäjille esimerkiksi SMS- tai sähköpostiviestillä, kun tietyt raja-arvot täyttyvät. Käytetty NetEyen versio tukeekin juuri näitä kahta tapaa lähettää tietoa halutessa eteenpäin.

Hälytyksistä lähtevä tieto konfiguroidaan NetEyessa erikseen määriteltyjen hälytysryhmien (Alert Group) kautta. Näihin hälytysryhmiin määritellään mitä tapahtuu, kun kyseinen ryhmä on asetettu hälytysryhmäksi testin tai laitteen asetuksissa. Ryhmään voidaan määritellä kenelle hälytyksistä lähtee tieto, ja mitä kautta se tapahtuu. Käytännössä ryhmään siis luetellaan sähköpostiosoitteet ja puhelinnumerot, joihin tieto hälytyksistä halutaan välittää. Erikseen voidaan vielä määrittää, kuinka kauan esimerkiksi ping-testin täytyy epäonnistua, ja ajankohdat, jolloin hälytykset ylipäätään läh-

tevät. Näillä voidaan varmistaa, ettei vain hetkellisistä ongelmista lähde turhaan viestejä eteenpäin, ja esimerkiksi viikonloput voidaan halutessa jättää hälytyksien ulkopuolelle. Kuviossa 20 on esitettynä hälytysryhmän konfigurointi-sivu.



Kuvio 20. Alert Group Management

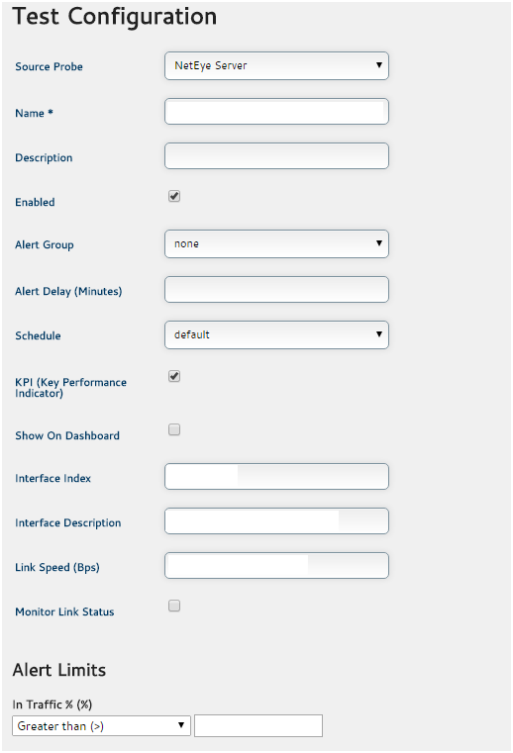
Tässä opinnäytetyössä päädyttiin lopulta siihen lopputulokseen, että kolmen valvotun tietoverkkolaitteen kohdalla on tarpeen käyttää näitä hälytysryhmiä. Käytännössä tämä tarkoitti sitä, että ensin luotiin tarvittava hälytysryhmä, minkä jälkeen tätä ryhmää voi käyttää jokaisen halutun laitteen tai testin yhteydessä. Luotuun hälytysryhmään lisättiin muutama sähköpostiosoite, joihin ongelmien ilmetessä viestit lähtee. SMS-viestien lähetystä ei puolestaan – ainakaan tässä vaiheessa – nähty tarpeelliseksi. Hälytysryhmät lisättiin kolmen tietoverkkolaitteen alle ja niiden valintaperusteena oli niiden kriittisyys tietoverkon toiminnan kannalta, pääpainon ollessa nimenomaan Puolan toimipisteen verkkoympäristössä. Ryhmä lisättiin laitteiden ICMP-Saatavuuskyselyn yhteyteen. Hälytykset konfiguroitiin siten, että viestit lähtevät eteenpäin, kun ping-testi ei ole mennyt läpi 15 minuuttiin. 15 minuutin aikamääre katsottiin sopivaksi rajapyykiksi kriittisyyden ja aiheettomuuden välimaastosta. Näitä arvoja on kuitenkin tulevaisuudessa helppo muuttaa ja vastaanottajalistan muokkaaminenkin onnistuu, jos se nähdään tarpeellisiksi.

6.4.3 SNMP-Interface

ICMP-kyselyiden lisäksi kahteen kytkimeen laitettiin, myös SNMP:n Interface-testi. Tällä kyselyllä voidaan tarkastella tietyn verkkorajapinnan läpikulkevaa liikennettä. Yleisesti tätä testiä käytetään nimenomaan liikenteen määrän tutkimiseen. Tästä voi olla hyötyä, kun esimerkiksi halutaan tarkastella, onko monitoroidun laitteen läpi kulkevan liikenteen määrä haluttua suurempi. Eli jos verkossa on ilmentynyt hitautta, voidaan interface-testin avulla tarkastella johtuiko hitaus yksinkertaisesti liian suuresta kaistan käytöstä vai onko ongelman lähdettä syytä etsiä toisaalta.

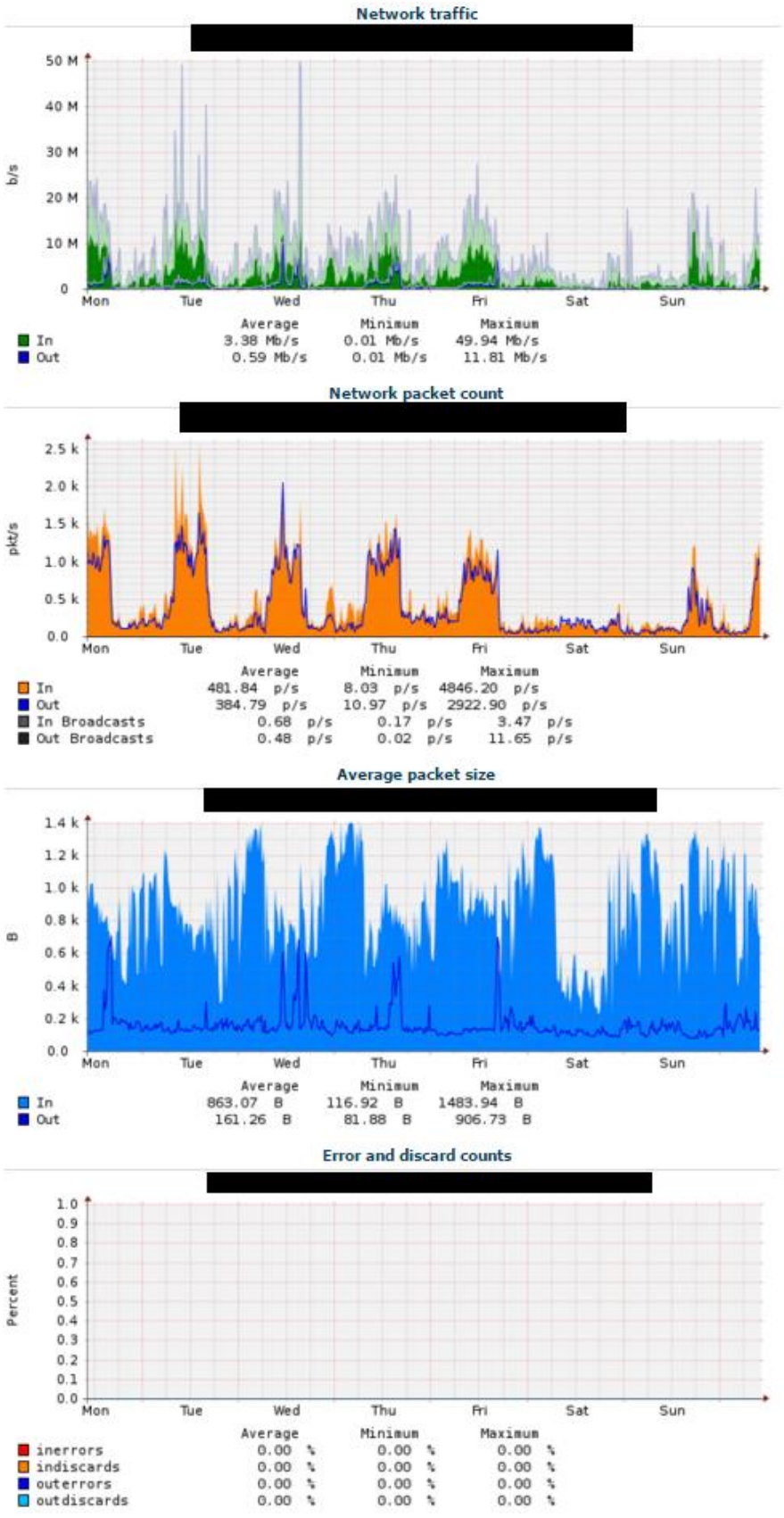
Verkkorajapintojen kohdalla hälytyksien raja-arvot laitettiin 90 % valitun verkkorajapinnan kapasiteetista. Tämä koskee, sekä ulospäin, että sisäänpäin kulkevaa liikennettä. Tähän arvoon päädyttiin lähinnä siksi, että se on NetEyen suosittelema oletusarvo, ja tutkimalla edellisten parin kuukauden statistiikkaa verkkorajapintojen tilanteesta havaittiin, että kyseiset arvot voivat hyvinkin ylittyä ja se voi aiheuttaa ongelmia.

Interface-testin lisääminen onnistuu NetEyen käyttöliittymästä muutamalla klikkauksella. Lisättäessä uutta testiä, NetEye skannaa laitteen kaikki verkkorajapinnat ja listaa ne käyttäjälle valittavaksi. Tästä listasta voidaan valita kaikki halutut kohteet,minkä jälkeen ne ilmestyvät valvontanäkymään muiden kyselyjen tapaan. Kuviossa 21 on Interface-testin konfigurointi-sivu.



Kuvio 21. Interface-test Configuration

Kun testit ovat lisättyinä halutuille laitteille, alkaa NetEye piirtämään kuvaaja valituiden laitteiden liikenteen määrästä. Näitä kuvaajia voidaan myöhemmin tutkia halutulta aikaväliltä ja ne voidaan tarvittaessa tallentaa muidenkin kuvaajien tapaan esimerkiksi pdf-tiedostoiksi. Kuviosa 22 on esitettynä toisen valvontaan asetetun kytkimen Interface-kyselyn palauttamaa dataa yhdestä verkkorajapinnasta.



Kuvio 22. Interface-testi

6.5 Palvelimien lisäys

Valvonnan alaisuuteen lisättiin tietoverkkolaitteiden lisäksi viisi eri palvelinta. Nämä palvelimet eivät fyysisesti sijaitse Puolan palvelukeskuksella, mutta ne ovat silti kriittisessä asemassa Puolan toimipisteen toiminnan kannalta. Palvelimia olisi voinut lisätä, vaikka useita kymmeniä, mutta se ei ollut tässä työssä tarkoituksenmukaista ja opinnäytetyön kannalta tietoverkkolaitteet olivat tärkeydeltään huomattavasti korkeammassa asemassa. Tavoitteena oli laittaa muutamia valittuja palvelimia valvontaan ja katsoa, että palvelimien monitorointi prosessina onnistuu vaivattomasti ja näin tulevaisuudessakin palvelimia voidaan tarvittaessa lisätä. Palvelimien valintojen tärkein kriteeri oli, että kyseessä on Puolan toimipisteen kannalta tärkeä palvelin. Tämän kriteerin pohjalta päädyttiin viiteen eri Windows-palvelimeen. Kolme valituista palvelimista (palvelimet P3, P4 ja P5) olivat kahden eri toimialueen AD-palvelimia, jotka ovat todella tärkeitä, koska palvelimet pitävät huolen, että toimialueille kirjautuminen onnistuu. Näiden lisäksi valvontaan laitettiin lisenssipalvelin P1, sekä imagepalvelin P2. Lisenssipalvelin on vastuussa luonnollisesti eli tuotteiden lisenssien jakelusta ja imagepalvelin pitää puolestaan pystyssä eri levykuvia, jotka ovat kovassa käytössä mm. Puolan toimipisteellä.

Palvelimienkin kohdalla ensimmäinen valvottava asia oli luonnollisesti laitteiden saatavuus. Tämä tarkoittaa sitä, että palvelimille annettiin täysin sama käsittely, kuin tietoverkkolaitteille käyttämällä ICMP:n saatavuus-kyselyitä.

Palvelimien lisääminen NetEyen valvonnan alle onnistuu täysin samalla kaavalla, kuin esimerkiksi reitittimien lisäys. Seuraavissa luvuissa on käyty tarkemmin läpi palvelimia ja niitä testejä, jotka lopulta näille palvelimille ajettiin.

6.5.1 ICMP-Testit

Palvelimienkin kohdalla ensimmäinen valvottava asia oli luonnollisesti laitteiden saatavuus. Tämä tarkoittaa sitä, että kaikille palvelimille annettiin tismalleen sama käsittely, kuin tietoverkkolaitteille käyttämällä ICMP:n saatavuus-kyselyitä. Jokainen palvelin piirtää täysin vastaavia kuvaajia, kuin tietoverkkolaitteet yllä, ja hälytykset muodostuvat samalla lailla NetEyen KPI-näkymään.

Palvelimien kohdalla toimeksiantaja katsoi, että hälytyksistä ei tarvitse erikseen lähettää sähköposteja tai SMS-viestejä käyttäen NetEyen hälytysryhmiä, joten ainakaan tässä vaiheessa hälytyksiä ei palvelimista ilmaannu, kuin NetEyen käyttöliittymään. Hälytysryhmät ovat toki todella helppo ja nopea lisätä jälkikäteen, jos se nähdään myöhemmin tarpeelliseksi.

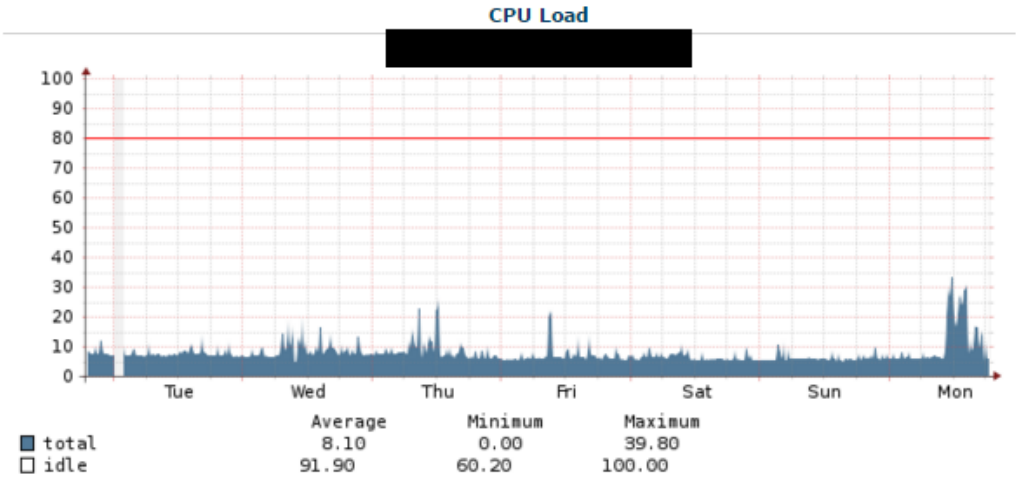
6.5.2 Prosessorin ja Muistin käyttöaste

Saatavuuskyselyjen lisäksi jokaiselle palvelimelle laitettiin SNMP-testit koskien CPU:n (Central processing unit) ja muistin käyttöastetta. Käyttöasteet saadaan testien avulla esitettynä prosentteina 0 – 100 %. Tieto fyysisen ja virtuaalisen muistin käyttöasteesta saadaan myös bitteinä, prosentuaalisen tiedon lisäksi. Hälytykset näistä testeistä muodostuvat, jos testit eivät mene ollenkaan läpi, tai annetut raja-arvot ylittyvät.

Vaikka valvonnan alle asetettujen palvelimien ei pitäisi suuren CPU:n ja muistin rasituksen alle, niin päädyimme kuitenkin nämä testit palvelimille asettamaan. Kuvaajista voidaan kuitenkin jälkikäteen tutkia, jos epänormaaleja tilanteita on ilmaantunut. Lisäksi, jos annetut raja-arvot käyttöasteiden osalta ylittyvät, on näiden palvelimien kohdalla todennäköisesti syytä huolestua.

Hälytyksien raja-arvoiksi asetettiin 80 %, sillä katsottiin, että valvonnassa olevien palvelimien käyttöasteet ei missään tilanteessa pitäisi nousta niin korkeaksi, joten tämän rajan ylittyessä on palvelimella todennäköisesti menossa jotain outoa. 80 % on lisäksi monesti verkonvalvonnassa käytetty oletusarvo, mikä pitää paikkansa myös NetEyen kanssa. Raja-arvojen ylityttyä, ilmaantuu niistä hälytys NetEyen käyttöliittymään, mutta hälytysryhmiä ei erikseen informoida sähköposteilla tai tekstiviesteillä.

Kuviossa 23 on esimerkki yhden CPU:n kuormasta viikon ajalta. Vastaava kuvaaja siis piirtyy jokaisen palvelimen muistin, sekä prosessorin käyttöasteesta.



Kuvio 23. CPU:n käyttöaste

6.5.3 AD-Palvelimet

P3,P4 ja P5 palvelimet ovat siis AD-palvelimia (Active Directory) ja näitä tarvitaan etenkin kirjautumiseen yrityksen toimialueisiin. Opinnäytetyön kannalta tärkeitä toimialueita on kaksi ja näistä vastaa palvelimet P3 ja P4. P5 on puolestaan P4-palvelimen varapalvelin ja ei näin ollen ole aivan yhtä kriittinen, kuin P4 itse. P5-palvelimella oli kuitenkin asennettuna SNMP valmiiksi, joten sen lisääminen valvontaan onnistui samalla vaivalla, kuin P4:n.

Saatavuuden ja prosessorin, sekä muistin käyttöasteen lisäksi AD-palvelimille lisättiin SNMP-testi ”Windows Services” eli Windows palvelut. Tällä testillä pystytään tarkkailemaan palvelimella olevien palveluiden tilaa. NetEye lähettää SNMP-kyselyn hallinta-agentille, joka vastaa listaamalla kaikki aktiiviset Windows-palvelut. Näistä palveluista voidaan valita kaikki palvelut, jotka halutaan monitoroitavaksi, ja jokaisesta valitusta palvelusta luodaan sitten oma testinsä. Jos valittu palvelu, tai itse hallinta-agentti ei vastaa, muodostaa NetEye siitä hälytyksen. Tähän testiin ei myöskään voi asettaa mitään raja-arvoja, koska ainut asia mitä tutkitaan, on palvelun aktiivisuus.

AD-palvelimien osalta tähän kyselyyn laitettiin Windows palvelut, jotka vastaavat nimenomaan Active Directoryn toiminnasta. Tällaisia palveluita ovat esimerkiksi ”Active Directory Domain Services”, sekä ”Active Directory Web Services”. Näiden testien avulla voidaan varmistaa, ettei palvelimien AD-palveluissa ole ongelmia, vaikka palvelin näyttäisi muuten olevankin kunnossa.

6.5.4 P1 ja P2 palvelimet

AD-kirjautumispalvelimien lisäksi valvontaan laitettiin P1-lisenssipalvelin sekä P2-imagepalvelin. Nämä palvelimet eivät kriittisyydeltään ole aivan korkeimmasta päästä, mutta ne kuitenkin päädyttiin – vähän testimielessäkin – lisäämään monitoroitavien laitteiden joukkoon.

Lisenssipalvelimen tehtävänä on nimensä mukaisesti pitää huolta eri sovelluksien ja palveluiden lisensseistä. Palvelin ei sinänsä ole äärimmäisen kriittinen sillä lisenssipalvelimen ongelmat harvemmin aiheuttavat todella kiireisiä tai laajoja ongelmia, mutta SNMP:n ollessa valmiiksi asennettuna, oli sen sisältäminen valvontaan järkevä ratkaisu.

P2 palvelin on puolestaan palvelin, joka pyörittää pääasiassa levykuvia (eli imageja). Jos tämä palvelin ei ole kunnossa, niin tietyt levykuvat eivät ole saatavilla, mikä saat-

taa vaikuttaa työntekoon laajassakin mittakaavassa. Nämä imaget ovat varsin kovassa käytössä varsinkin Puolan toimipisteellä, joten tämän palvelimen lisäys monitoroitavaksi oli varsin looginen ratkaisu.

Molemmille palvelimille tehtiin samankaltaiset toimenpiteet, kuin AD-palvelimille. Ensimmäisenä tehtiin ICMP-saatavuuskyselyt ja käyttöasteiden tarkastelu samalla kaavalla, kuin kappaleissa 6.5.1 ja 6.5.2 esitettiin. P1 palvelimelle tehtävät testit jätettiin näihin kolmeen ja P2 sai näiden lisäksi vielä AD-palvelimienkin kanssa käytetyn Windows palvelut-testin. Lisenssipalvelimen kohdalla ei nähty tarpeelliseksi palveluiden tilannetta niiden epäkriittisyyksien vuoksi. Imagepalvelimen kohdalla valvontaan laitettiin AD-palvelimien tavoin Windows palvelut, jotka ovat vastuussa levykuvien toiminnasta.

6.6 Käyttäjäryhmät

Itse valvonnan lisäksi NetEye tarjoaa mahdollisuuden muodostaa eri käyttäjäryhmiä eri oikeuksilla. Käytännössä tämä tarkoittaa sitä, että tietylle käyttäjäjoukolle voidaan antaa oikeudet tarkastella vain osaa valvotuista laitteista, ja esimerkiksi estää kyseiseltä joukolta kaikki ylläpidolliset ominaisuudet. Käyttäjäryhmiin voidaan helposti valita profiilien puurakenteesta halutut puut tai oksat, jotka tulevat näkymään käyttäjäryhmän alle määriteltyjen käyttäjien lopullisessa päänäkymässä.

Tämän opinnäytetyön yhteydessä päädyttiin tekemään toistaiseksi vain yksi ryhmä, johon lisättiin tässä vaiheessa kaksi eri käyttäjätunnusta. Tällä ryhmällä on oikeudet tarkastella aktiivisen valvonnan alla olevia laitteita ja niiden piirtämiä käyriä ilman ylläpidon ominaisuuksia. Esimerkiksi uusien laitteiden lisääminen tai olemassa olevien laitteiden muokkaaminen ei onnistu.

Käyttäjäryhmälle asetettiin näkyviin sama puunäkymä, joka aiemmin määritettiin kappaleessa 6.2. Tämä käyttäjäryhmä luotiin, koska nähtiin, että on tarpeellista olla

olemassa myös käyttäjiä, jotka pystyvät tarkkailemaan hälytyksiä, mutta eivät toisaalta taas pysty sotkemaan olemassa olevaa järjestelmää. Tällä hetkellä itse käyttäjiä tälle ryhmälle luotiin todellakin vain kaksi kappaletta, mutta niiden lisääminen jälkikäteen on todella helppoa, käyttäjäryhmän ollessa valmiiksi luotuna ja konfiguroituna.

7. Pohdinta

Tämän opinnäytetyön perimmäisenä tavoitteena oli ottaa alustavasti käyttöön Qentinel NetEye verkonvalvonta ohjelmisto, joka oli jo valmiina hankittuna toimeksi antavan yrityksen toimesta. Tämä projekti nähtiin tarpeelliseksi tukemaan osaksi jo olemassa olevaa valvontaa, sillä kyseessä on varsin suuri yritys ja NetEyen avulla saadaan yksi valvonnan osa lisää helpottamaan - varsinkin Puolan toimipisteen - verkon valvontaa. Verkon ylläpito ja valvonta Baronan kokoisessa yrityksessä onkin hyvin laaja ja monimutkainen käsite, joten tässä opinnäytetyössä keskityttiin nimenomaan Puolan palvelukeskuksen toimintaan vaikuttaviin laitteisiin.

Ennen varsinaisen käytännön työn aloitusta oli syytä hankkia vahva tietoperusta aiheesta. Verkkovalvonta oli käsitteenä ennen työn alkua täysin tuntematon, joten pohjatyötä sai tehdä runsaasti, jotta peruskäsitteet alkoivat olla hanskassa. Kirjallisuutta verkonvalvonnasta löytyi varsin niukasti, mutta lopulta muutamien kirjojen ja standardien pohjalta saatiin kasaan hyvä yleiskuva verkonvalvonnan perusteista ja toiminnoista.

Kun tietoperusta oli hankittu, ja verkonvalvonnasta alkoi olemaan hyvä käsitys, oli aika alkaa miettimään itse käytännön osuutta NetEyella toteutettuna. Aluksi tuli kartoittaa, millainen ohjelmisto NetEye oikein on ja mitä sillä voidaan tehdä. Tässä operaatiossa auttoi NetEyen omat ohjeet, sekä Qentinelin edustajan kanssa käydyt keskustelut, joiden jälkeen NetEyen mahdollisuudet alkoivat selvitä, ja se lopulta paljastuikin varsin yksinkertaiseksi ja helppokäyttöiseksi järjestelmäksi.

Käytetyn ohjelmiston ollessa tuttu, tuli seuraavaksi päättää, mitä valvotaan, ja miten valvotaan. Yhdessä toimeksiantajan kanssa kartoitimme eri mahdollisuuksia, ja lopulta valitsimme yhteensä 10 eri valvottavaa kohdetta, jotka ovat läheisessä tekemisissä nimenomaan Puolan toimipisteen kanssa. Valvottavien laitteiden lisäksi päätettiin lisäksi, mitä näistä laitteista oikein valvotaan, kuinka hälytyksiä käsitellään jne.

Itse valvottavien laitteiden lisääminen oli todella mekaanista suorittamista. Ongelmat koostuivatkin lähinnä pohjatyöstä, koska tämänkin kokoisen yrityksen verkkotopologia on varsin monimutkainen ja laaja. Niinpä valvonnan toteutusta tehdessä jouduttiin konsultoimaan muutamia eri osapuolia, että valvontaan lisättävistä laitteista saatiin tarvittavat tiedot kasaan. Kun valvottavat laitteet olivat valittu ja tarvittava data yhteisönimineen selvillä, oli laitteiden lisäys valvonnan piiriin yksinkertainen prosessi. Varsinkin, kun NetEye alkoi työkaluna olla tuttu, tapahtui uusien valvottavien laitteiden lisäys todella vaivattomasti ja nopeasti.

Kokonaisuutena opinnäytetyössä päästiin siihen lopputulokseen, johon pyrittiin: Qentinel NetEyen käyttöönotto painottaen Puolan toimipisteen verkkoa. Tämän projektin pohjalta on helppo lähteä jatkamaan ja laajentamaan NetEyen piiriin asetettua valvontaa, sikäli kun se tulevaisuudessa nähdään tarpeelliseksi. Itse valvonnan toteutus oli lopulta varsin suoraviivainen projekti, ja suurimmat ongelmat olivatkin suunnittelun ja valmistelun kanssa, eikä niinkään itse valvottavien laitteiden lisäämisessä. Haasteita aiheutti myös yrityksen tietoverkkoliikenteen arkaluontoisuus, minkä takia pääsy tietoverkkolaitteisiin oli hyvin rajattua. Käytännön puolta olisi ollut mukava päästä tekemään jopa enemmän aivan verkkolaitteiden SNMP:n konfiguroinnista lähtien, mutta tämä ei ollut mahdollista toimeksi antavan yrityksen järjestelyistä johtuen. Kuitenkin tekemistä riitti, ja lopulta saatiin aikaiseksi toimiva paketti, jonka pohjalta on hyvä lähteä jatkamaan verkonvalvonnan loputonta prosessia.

Lähteet

Barona yrityksenä. N.d. Tiivistelmä Barona Group Oy:n sivustolla. Viitattu 6.12.2015 https://www.barona.fi/yrityksille/barona-yrityksena

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Diplomityö. Aalto-yliopiston teknillinen korkeakoulu, Tietotekniikan osasto http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/thesis.html

ICT-palveluratkaisut. N.d. Artikkeli Barona Group Oy:n sivustolla. Viitattu 6.12.2015 https://www.barona.fi/yrityksille/tehokkuutta/ICT-Service-Desk

ISO/IEC 10040. 1997. Information technology - Open Systems Interconnection - Systems management overview http://www.itu.int/rec/T-REC-X.701-199708-I

ISO/IEC 7498-4. 1989. Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework http://standards.iso.org/ittf/PubliclyAvailableStandards/

ITU-T x.700. 1992. http://www.itu.int/rec/T-REC-X.700-199209-I/en

Jaakohuhta, H. 2002. Lähiverkot – Ethernet. Helsinki: Edita.

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo Finland Oy

Mauro, D. & Schmidt, K. 2005. Essential SNMP, 2nd Edition. O'Reilly Media

Nash, K. & Behr, A. 2007. Network Monitoring Definition and Solutions. Artikkeli CIO:n sivustolla verkkomonitoroinnin perusteista. Viitattu 25.8.2015 http://www.cio.com/article/2438133/networking/network-monitoring-definition-and-solutions.html

Qentinel NetEye - Näkyvyyttä ICT-palveluihin. N.d. Qentinel Oy:n tiivistelmä NetEye palvelusta. Viitattu 18.9.2015. http://www.qentinel.com/fi/qentinel-neteye-naekyvyyttae-ict-palveluihin

Qentinel NetEye 4.1.0 Administrator manual. 2013. Qentinel Oy:n kirjoittama ylläpitomanuaali.

RFC 1757. 1995. Remote Network Monitoring Management Information Base http://www.ietf.org/rfc/rfc1757.txt

RFC 2021. 1997. Remote Network Monitoring Management Information Base Version 2. http://www.ietf.org/rfc/rfc2021.txt

RFC 792. 1981. Internet Control Message Protocol http://www.ietf.org/rfc/rfc792.txt